U.S. Army Research Institute
for the Behavioral and Social Sciences

Research Report 1550

Doing Deception: Attacking the Enemy's Decision Processes

James H. Hicinbothom and Wayne W. Zachary
CHI Systems, Inc.

Beverly G. Knapp
U.S. Army Research Institute

Allen L. Zaklad, Alvah C. Bittner, Jr., and Alfons L. Broz
Analytics, Inc.

February 1990

U.S. ARMY RESEARCH INSTITUTE
FOR THE BEHAVIORAL AND SOCIAL SCIENCES

A Field Operating Agency Under the Jurisdiction of the Deputy Chief of Staff for Personnel

EDGAR M. JOHNSON
Technical Director

JON W. BLADES
COL, IN
Commanding

Research accomplished under contract
for the Department of the Army

Analytics, Inc.

Technical review by

David D. Burnstein
Herny Trosper, U.S. Army Intelligence Center and School

NOTICES

DISTRIBUTION: Primary distribution of this report has been made by ARI. Please address correspondence concerning distribution of reports to: U.S. Army Research Institute for the Behavioral and Social Sciences, ATTN: PERI-POX, 5001 Eisenhower Ave., Alexandria, Virginia 22333-5600.

FINAL DISPOSITION: This report may be destroyed when it is no longer needed. Please do not return it to the U.S. Army Research Institute for the Behavioral and Social Sciences.

NOTE: The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS --
2a. SECURITY CLASSIFICATION AUTHORITY --	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE --	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) TR 2074-3	5. MONITORING ORGANIZATION REPORT NUMBER(S) ARI Research Report 1550
6a. NAME OF PERFORMING ORGANIZATION Analytics, Inc.	6b. OFFICE SYMBOL (If applicable) --
7a. NAME OF MONITORING ORGANIZATION U.S. Army Research Institute Field Unit at Fort Huachuca	
6c. ADDRESS (City, State, and ZIP Code) 2500 Maryland Road Willow Grove, PA 19090	7b. ADDRESS (City, State, and ZIP Code) Fort Huachuca, AZ 85613-7000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION U.S. Army Research Institute for the Behavioral and Social Sciences	8b. OFFICE SYMBOL (If applicable) PERI-S
	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER MDA903-86-C-0403
8c. ADDRESS (City, State, and ZIP Code) 5001 Eisenhower Avenue Alexandria, VA 22333-5600	10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
62785A	790	1306	C3

11. TITLE (Include Security Classification)
Doing Deception: Attacking the Enemy's Decision Processes

12. PERSONAL AUTHOR(S) Hicinbothom, James H., Zachary, Wayne W. (CHI Systems); Knapp, Beverly G., (ARI); Zaklad, Allen L., Bittner, Alvah C., Jr., and Broz, Alfons L. (Analytics, Inc.)

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM 88/05 TO 89/05	1990, February	

16. SUPPLEMENTARY NOTATION
Beverly G. Knapp, Contracting Officer's Representative
CHI Systems is the subcontractor for this research.

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Deception; Deception planning; Military deception; Battlefield deception; Tactical deception; Deception vulnerability; (Continued)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This report examines military deception from the point of view of the battlefield deception planner. Tactical decision cycles are surveyed and basic concepts for deceiving them are presented. These concepts are applied to the deception planning process, resulting in an enhanced planning process that builds upon current doctrine. Tactical examples are offered to illustrate this approach.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
Beverly G. Knapp	(602) AV 879-4704	PERI-SA

DD Form 1473, JUN 86 *Previous editions are obsolete.*

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

ARI Research Report 1550

18. SUBJECT TERMS (Continued)

OPFOR deception cycle,
Pathfinding,

(Opposing force)

Accession For	
NTIS GRA&I	☑
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

Research Report 1550

Doing Deception: Attacking the Enemy's Decision Processes

James H. Hicinbothom and Wayne W. Zachary
CHI Systems, Inc.

Beverly G. Knapp
U.S. Army Research Institute

Alan L. Zaklad, Alvah C. Bittner, Jr., and Alfons L. Broz
Analytics, Inc.

Field Unit at Fort Huachuca, Arizona
Julie A. Hopson, Chief

Systems Research Laboratory
Robin L. Keesee, Director

U.S. Army Research Institute for the Behavioral and Social Sciences
5001 Eisenhower Avenue, Alexandria, Virginia 22333-5600

Office, Deputy Chief of Staff for Personnel
Department of the Army

February 1990

Army Project Number
2Q162785A790

Human Performance Effectiveness and Simulation

FOREWORD

The Fort Huachuca Field Unit of the U.S. Army Research Institute for the Behavioral and Social Sciences (ARI) performs research in key areas of interest to the U.S. Army Intelligence Center and School (USAICS). One such area is battlefield deception. In the research reported here, ARI uses the results and methods of cognitive and organizational psychology to support the development of battlefield deception training and doctrine.

Deception can serve as a powerful force multiplier for engaging a numerically superior opposing force (OPFOR). Historically, military deception has been practiced as an art; little systematic "how-to" guidance has been available. This report contributes to the scientific understanding of battlefield deception by analyzing the OPFOR decision-making process and providing approaches to manipulating this process with deception. Products of this research will be tools and aids for the deception planner, trainer, and developer of doctrine.

EDGAR M. JOHNSON
Technical Director

DOING DECEPTION: ATTACKING THE ENEMY'S DECISION PROCESSES

EXECUTIVE SUMMARY

Requirement:

To support the more effective use of battlefield deception by Army personnel by developing cognitively-based approaches, tools, and aids for the deception planner, trainer, and developer of doctrine.

Procedure:

The concept of battlefield deception was developed and an enhanced deception process was constructed that builds upon current doctrine. To provide a basis for the enhanced planning process, the military decision-making cycle of the opposing force (OPFOR) was characterized and compared with that of the friendly force (FFOR). Two illustrations of deception pathfinding were presented in the context of an OPFOR attack across the Inter-German border.

Findings:

The FFOR and OPFOR decision cycles were *summarized* and compared with respect to vulnerability to deception. Key concepts were identified and organized into deception means, deception method, and deception criteria. *Pathfinding*—analysis of the vulnerability to deception of a given segment of the OPFOR decision cycle—was defined and applied to enhance the deception planning process. Tactical examples of this approach were presented.

Utilization of Findings:

The products of this research will provide practical benefits as well as a basis for the systematic understanding of deception. In the near term, this research will provide a foundation for an enhanced deception process that builds upon current doctrine in FM 90-2. In the long term, this research may be expected to lead to approaches, tools, and aids for deception planners, trainers, and doctrine developers.

DOING DECEPTION: ATTACKING THE ENEMY'S DECISION PROCESSES

CONTENTS

LIST OF TABLES

LIST OF FIGURES

DOING DECEPTION: ATTACKING THE ENEMY'S DECISION PROCESSES

This document discusses battlefield deception in the operational-tactical sphere, focusing primarily on the corps-division levels. Initially, it examines the role of deception in the modern Army, and the military decision making process which deception attempts to attack. Subsequently, it considers how the OPFOR decision cycle may be disrupted. Tactical examples of this approach are presented to illustrate some of its many applications.

DECEPTION IN THE MODERN ARMY

What is deception and how does it fit into the way the U.S. Army fights?

Military deception is a highly specialized, discreet, and sophisticated art of warfare. Throughout history, it has successfully supported and enhanced victorious efforts on the battlefield. In recent years, battlefield deception has gained increasing attention as a potential "force multiplier" and an effective way of "fighting smarter." The need for utilizing force multipliers and fighting smarter has grown out of recognition of the nature of the threats now facing the U.S. Army. The charter for battlefield deception stems directly from the AirLand Battle Doctrine, which was formulated in response to these threats. Defense Science Board studies (1982-1983), which in part led to today's AirLand Battle Doctrine, have recommended that battlefield deception be a systematic, integral part of overall decision making and planning. These studies also recommended that it should be consistent with both: (1) Command, Control and Communications Countermeasures (C3CM) operations, and (2) Operations Plans that incorporate deception at echelons above corps (EAC).

Deception is one member of the family of C3CM activities which also includes Electronic Warfare (EW) and Operations Security (OPSEC). EW focuses on attacking the OPFOR's command and control systems, primarily through affecting electronic communications systems and electronic intelligence-gathering devices. OPSEC focuses on denying information, where possible, and controlling information about FFOR capabilities and intentions which might be of value to the OPFOR. Deception planning, as is true with most C3CM activities, is primarily the responsibility of the operational planners in the G-3 section's Deception Cell. However, support for their planning requires considerable interaction with the G-2 section (Intelligence). Deception functions properly only if the staff elements involved fully coordinate their efforts toward support of their commander's decision making.

Battlefield deception is basically the process of misrepresenting the battlefield situation or friendly force (FFOR) capabilities and intentions. The purpose of this misrepresentation is to induce the opposing force (OPFOR) into behaving in a way desirable to the FFOR. Battlefield deception may be viewed as being based on solving five key problems:

(1) Determining how the FFOR wants the OPFOR to act;

(2) Understanding what perceived situation would cause the OPFOR commander to act in the specified desirable way;

(3) Determining what information and intelligence, from what sources, would get the OPFOR commander to perceive the battlefield situation in the desired way;

(4) Understanding how to manipulate the intelligence data collected by the OPFOR to cause the OPFOR commander to get the desired information and intelligence from the necessary sources; and, as always,

(5) Determining how to use the resources available to the FFOR to manipulate that data as desired.

These five problems are implicit in the analyses of battlefield deception which are presented in this report.

The challenge of conducting battlefield deception is to find a practical, resourceful way to integrate all essential capabilities and bring them to bear on the OPFOR. A major step toward solving this problem

was the codification of U.S. Army doctrine in *Field Manual 90-2, Battlefield Deception.* The doctrine outlined in this manual is a necessary beginning, but is limited in its scope: FM 90-2 outlines "what" needs to be done, but does not detail "how." The "how" requires understanding OPFOR decision cycle vulnerabilities and then devising a deception plan that exploits these vulnerabilities through "enhanced deception planning". The goal of this report is to show how one develops and then uses enhanced deception planning in a battlefield situation.

MILITARY DECISION MAKING

If deception is attacking the enemy's decision making processes, what are these processes, and how do they function?

Decision making and coordinated execution of those decisions are the heart and soul of success on the battlefield. Making the right decisions and executing them in a timely, well-coordinated manner requires accurate intelligence and information about: the enemy, the battlefield situation, and one's own forces. This is where deception becomes so important -- if inaccurate or misleading information is used even by an excellent decision maker, the resulting decision will be inappropriate for the real battlefield situation. It is therefore important to understand how misleading information affects the decision making of a military unit. This section outlines the functional roles and decision cycle of a generic OPFOR.

The Commander

An OPFOR commander is responsible for all decisions made in his unit. Even when he delegates authority to key staff members, the final responsibility rests with him. The commander must carry out a delicate balancing act. He must not lose sight of the "big picture" of his overall mission by getting caught up in the details of making, implementing and executing his plans (not seeing the "forest" for the "trees"). On the other hand, he must not get so caught up in viewing the big picture that he loses sight of the critical details which spell success or failure for his grand plans (seeing the forest but not the tree falling toward him). The commander must rely on his staff and his subordinate units to help him maintain this balance: to look at the details when appropriate as part of an integrated view of the battle. The disruption of this balance is the goal of battlefield deception: *careful manipulation of information reaching the OPFOR commander may provide significant advantages to the FFOR.*

The Staff

An OPFOR staff are responsible for identifying, evaluating, and managing the flood of specific details involved in military operations. Most military organizations have a principal core of staff, usually directed by the Operations staff officer or the Chief of Staff, who provide the most direct support to the commander. Their primary purpose is to direct his attention to critical details affecting the mission, while not distracting him from the big picture. Not only must the staff get the details right, but they must also understand how the details affect the management of the whole battle. The commander must help them understand how the details of their mission affect the overall success or failure of the next higher echelon's mission. They function as integrators of information and intelligence, as filters for information going to the commander, and as planners who implement the commander's decisions and help him manage the execution of those plans. The OPFOR staff is both the most significant obstacle to deception and its strongest ally.

The Information Sources

There are a variety of information sources which provide critical information to the commander of an OPFOR. These sources consist mainly of intelligence units, logistics units, maneuver units, and fire units subordinate to the commander, though some significant intelligence and information is also available from higher echelons. The most critical sources of intelligence and information are the organic and attached intelligence collection assets, through the Intelligence staff section. In addition, the staff provide information about the expected impact of weather and terrain on the battle; the combat units, through the Operations staff section, about the current battlefield situation and the status of OPFOR units and assets;. the combat support units, through their special staff sections, about their capabilities to support the mission; and the service support units, through the Logistics staff section, about personnel, supplies, and

the lines of communication needed to support the mission. The OPFOR's information sources are the medium for his deception.

Engaging the Enemy

Once a decision is made, objectives set, and plans deconflicted and distributed, the combat and combat support units must execute the plan and engage the enemy. While engaging the enemy, the need for continued communication and guidance becomes critical. The first casualty of any engagement is often the plan for that engagement. Fragmentary orders are created by the commander (and his staff) to supplement or replace elements of the operations order which described the plan and guided its execution. How a military organization handles this problem of adapting and refining plans "on the fly" in battle is critical to its success. This places a burden on the information sources, the staff, and the commander, to say nothing of the subordinate combat units.

C2 Decision Making Processes

Battlefield decision makers act on their beliefs about the current and projected battlefield situation. Therefore, the processes by which they build their view of the situation are of crucial importance to deception planners. The means by which the enemy organization collects data, builds intelligence out of it, and plans actions based upon it is their C2 decision making process (or decision cycle). A decision cycle can be viewed as a set of five inter-connected subordinate processes:

- Sense, or the *data collection* process — collection of data about the FFOR through use of various sensors, including data reported by troops involved in engagements with the FFOR;
- Analyze and Integrate, or the *intelligence production* process — analysis and consolidation of data resulting in the production of intelligence of interest to the commander;
- Evaluate and Decide, or the *decision making* process — evaluation of available intelligence and of plans and orders imposed from higher echelons resulting in command decisions;
- Plan and Supervise Course of Action, or the *action control* process — the use of intelligence regarding the FFORs' capabilities, resources and intentions, along with OPFOR's objectives, capabilities, and resources, to plan and supervise the details of courses of action to achieve the mission objectives; and
- Act, or the *execution* process — carrying out the selected course of action under the supervision of the action control process.

These five processes interlock within each echelon to form one continuous information-processing cycle, as shown in Figure 1. Information flows up the left side of this structure until it reaches the Evaluate and Decide process. There it forms the information about the situation upon which the commander bases his decisions. Once the commander formulates goals and constraints for a course of action, these goals and constraints cascade down the right side of the structure in the form of plans and orders which are further refined and finally executed in the Act process. It is important to note that each process has its own decision makers: (1) individuals who decide what data meets the selection criteria; (2) others who decide which pieces of information fit together as part of the same big picture of the battlefield; and (3) still others who decide which of their observations would be of interest to higher elements.

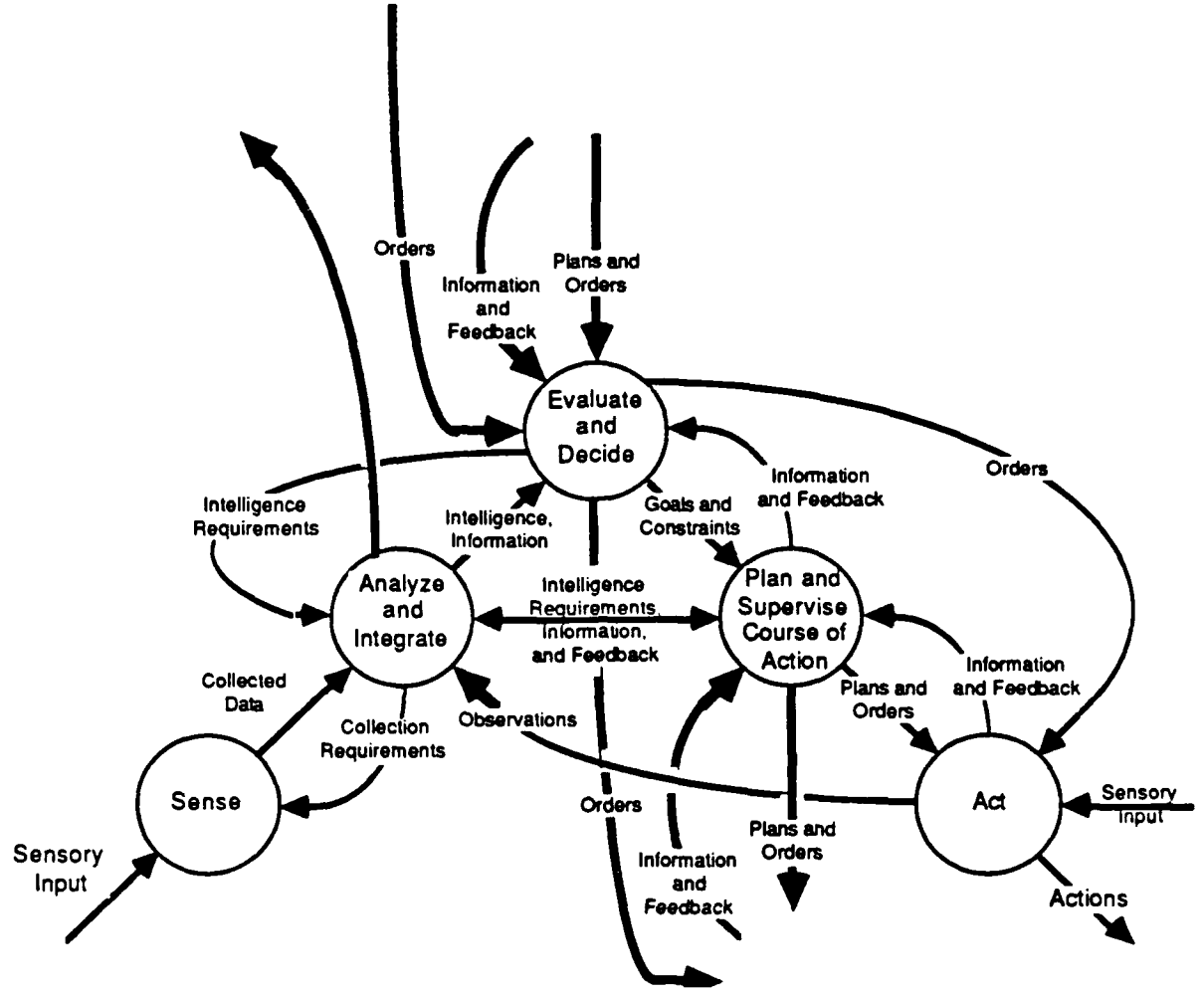


Figure 1. Intra-echelon information processing.

OPFOR decision makers and the units they command do not operate with total independence as might be deduced from the above description of military decision making. Figure 2 shows that these units form elements of a larger organization (e.g., front or corps) studying, planning, and controlling the battle. By viewing the decision cycle shown in Figure 1 as an intermediate echelon within a larger military structure, this fact can be most readily appreciated. The echelon in question could be a Soviet combined arms army (middle ellipse), superior to several tank and motorized rifle divisions (represented by the bottom ellipse), and subordinate to a front (top ellipse).

Thus a military organization can be viewed at many levels: (1) as an independent unit; (2) as a unit dependent on immediate superiors and subordinates; or (3) as a portion of a larger, more complex military organization (represented by adding additional echelons). There will usually be several adjacent units at a given echelon within a larger organization, rather than the single unit represented for each echelon in Figure 2. Understanding these diverse levels is necessary to get the right misinformation to the appropriate decision makers.

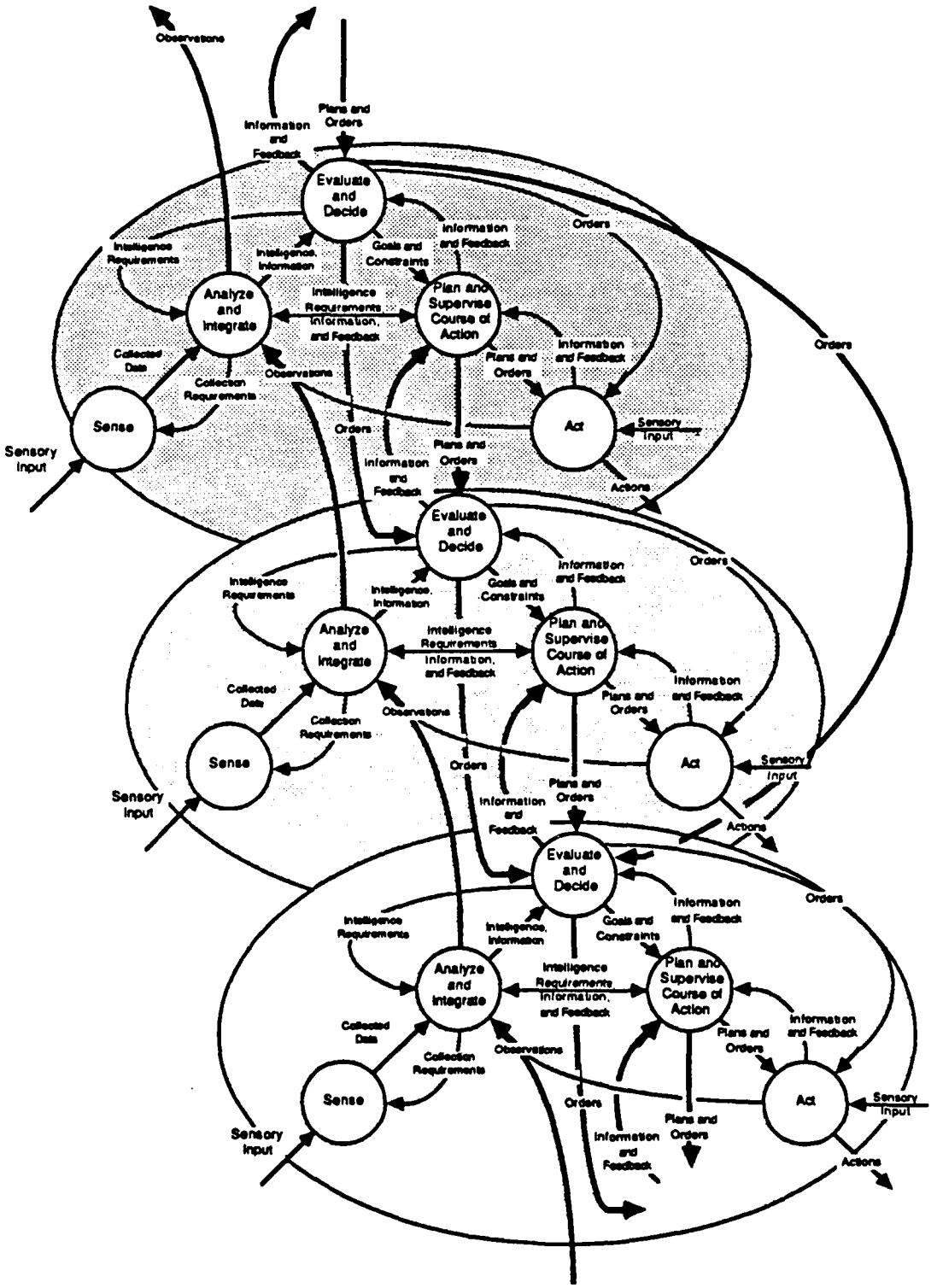


Figure 2. Inter-echelon information processing.

FFOR AND OPFOR DECISION MAKING PROCESSES

What do these decision making processes look like in real military organizations -- surely they are not the same in all organizations?

In order to understand the deception function, it is also necessary to understand the decision making processes of the FFOR and the OPFOR. This section presents brief descriptive analyses of these decision cycles for both US Army forces (FFOR) and Soviet Army forces (OPFOR). Although the terminology used by the two sides is often similar, frequently there are significant differences in meaning. Significant similarities and differences between the decision cycles are outlined at the end of this section.

FFOR Decision Cycle

Decision making in the friendly force will be examined at two levels: how a given unit makes its decisions, and how decision making takes place between echelons. These two levels are examined below in the order given.

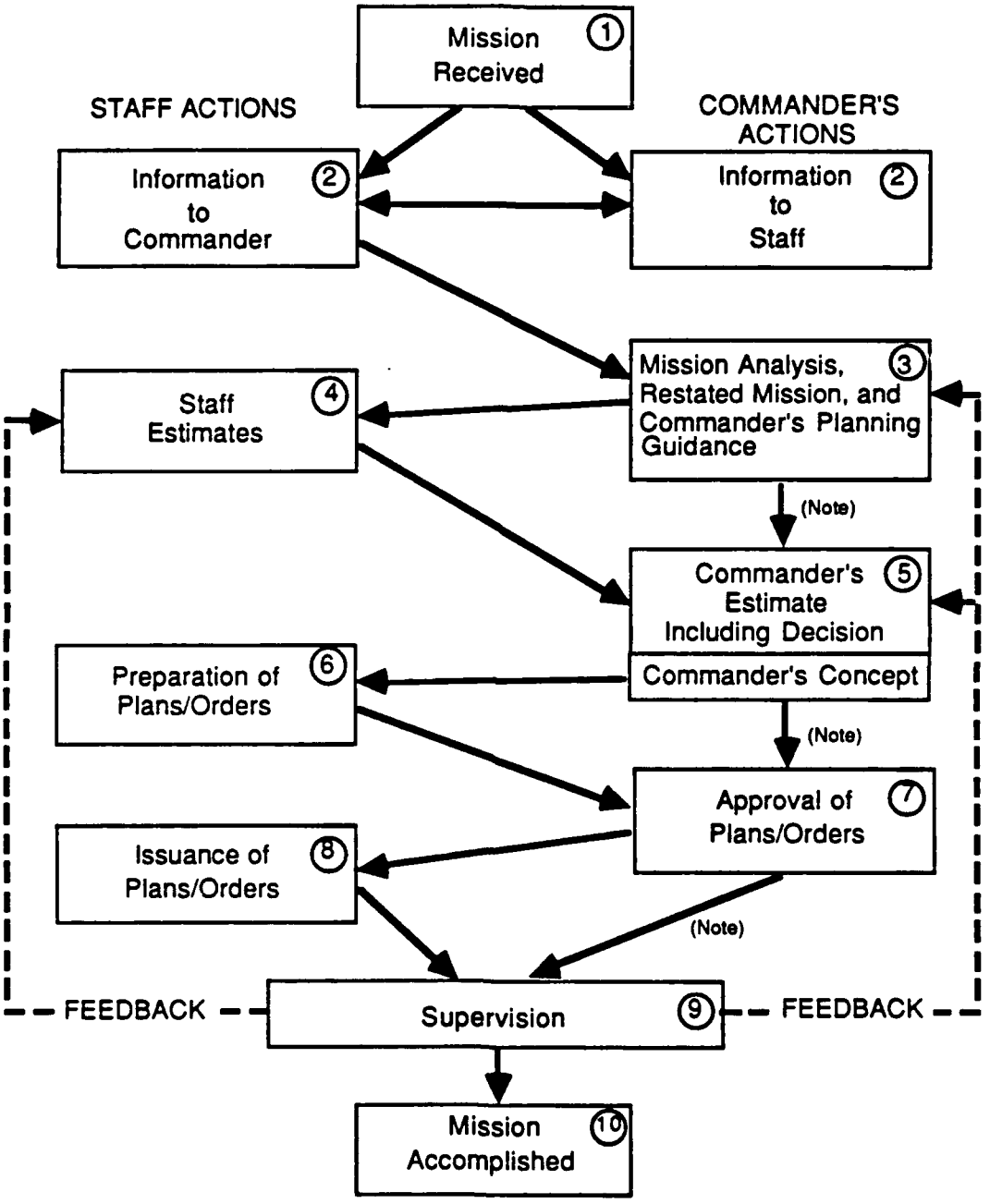
Decision Making Process Within an Echelon.

The FFOR decision cycle within an echelon begins with the receipt of a mission as laid-out in *FM 101-5 "Staff Organization and Operations"* (Headquarters, DA, 1984). Figure 3 illustrates this intra-unit decision making process. Once a mission is received (Step 1), the commander and his staff exchange information (Step 2) about the METT-T factors (Mission, Enemy, Terrain, Troops, and Time). The commander then issues planning guidance and a restatement of the mission to his staff; a potential course of action is outlined presenting his initial intent for accomplishing the mission (Step 3). Based on this guidance, the staff prepare their estimates of the situation (Step 4).

The commander receives his staff's estimates and analyzes them (Step 5). He decides upon a more detailed course of action, formulates his concept for accomplishing the mission, and disseminates it to his staff and subordinates. During this phase, he formalizes the objectives of the mission and specifies the major constraints under which it must be achieved.

Next the coordinating staff prepare plans and orders for implementing the commander's concept (Step 6). At this critical point, all constraints must be examined in detail and any conflicts resolved. Once an Operations Plan (OPLAN) or Order (OPORD) and an Administrative/Logistic Plan (Admin/Log PLAN) or Order (Admin/Log ORDER) have been formulated, they are presented for final review and approval to the commander. Before they are approved, he is responsible for examining them in terms of the big picture (Step 7). Then the Chief of Staff and the Assistant Chief of Staff for Operations (G3) record and issue the approved plans and orders (Step 8).

The various control measures built into the plans and orders must be monitored as they are executed by subordinate units (Step 9). Decisions must be made about how the course of action should be adjusted as the battlefield situation changes and control measures are triggered. Finally, the mission is accomplished (Step 10).



NOTE: In time-critical situations, the commander may be forced to complete his estimate based on his personal knowledge of the situation and issue oral orders to his subordinate units.

Figure 3. Intra-echelon decision-making process.

Decision Making Interactions Between Echelons.

"Inter-echelon" decision making takes place in a very complex, rapidly changing environment. Each echelon depends upon its subordinates and superiors for critical assistance in accomplishing its mission. AirLand Battle doctrine requires inter-echelon decision making to provide rapid, coordinated and appropriate responses by the whole FFOR. This process is based upon the hierarchical organization of the FFOR, as shown in Figure 4. Each echelon receives its mission from the echelon immediately above it, and feedback, information, and intelligence about the battlefield situation from units in echelons subordinate to it. This data is filtered, analyzed, and consolidated by the staff and then brought to the attention of the commander who uses it to formulate his next response.

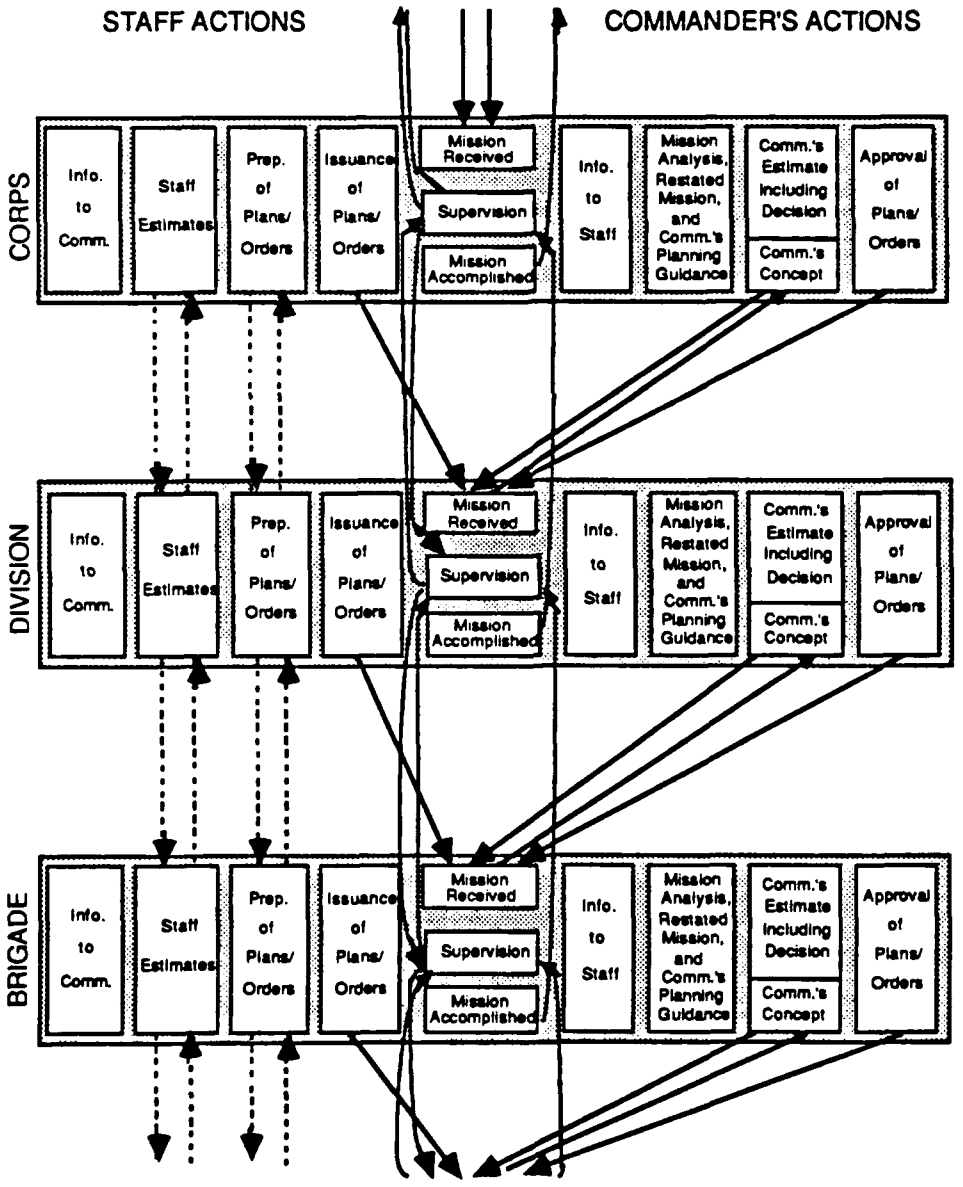


Figure 4. Inter-echelon decision-making process.

The principal interactions between echelons which influence the commander's decisions take three forms:

- Form 1 -- decisions cascade down the chain of command, with each echelon making plans in response to the mission assigned by the superior echelon;
- Form 2 -- information and intelligence about the enemy flow upwards through the echelons, so that higher echelon commanders have the information they need to manage the battle; and
- Form 3 -- subordinate commanders inform their superiors about their status (e.g., progress toward their objective, remaining resources, and assets and capabilities estimated to be available for future actions).

OPFOR Troop-Control System and Decision Cycle

The OPFOR troop-control system may be viewed as a distinctly structured, but functionally-oriented hierarchy as seen in Figure 5.

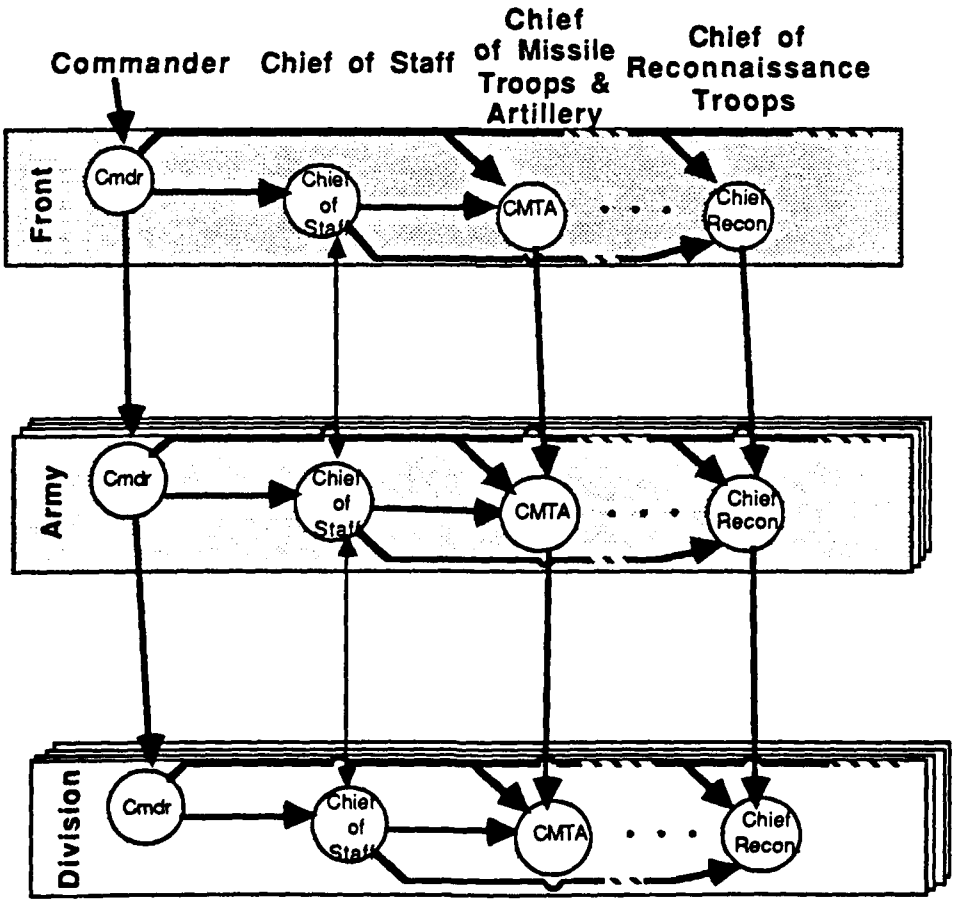


Figure 5. OPFOR troop-control system.

Inter-Echelon Troop Control System.

The Division Commander receives his direction primarily from his Army Commander and directs his subordinate regiments through their commanders. However, the Front Commander can exercise "skip-echelon" control, commanding the Division Commander directly. The Army Commander may likewise directly control the Division's Regiments. This principle of centralized "one-man management" is inherent in the structure of the OPFOR decision cycle and troop-control system.

The Division Commander controls the staff elements within his echelon primarily through his Chief of Staff. As shown in Figure 6, the Chief of Staff is a major player in each echelon. He coordinates and provides control for various staff members, including the Chief of Missile Troops and Artillery (CMTA) and the Chief of Reconnaissance Troops. This control is balanced by that exerted by corresponding functional elements of superior echelons. In particular, the CMTA receives functional direction from the higher echelon's (Army) CMTA. Likewise, the Chief of Reconnaissance Troops, as well as the other functional staff elements, receive functional direction from their higher echelon's corresponding functional elements. This functional direction may supercede the Division Commander's when functional control is exerted directly from the commander of the higher echelon. In similar fashion, the functional staff elements of both the superior Army and subordinate Regiment of Commanders may be controlled functionally through their respective higher echelons (i.e., Front and Division). OPFOR higher echelons appear to have more direct, rapid, and precise control over individual lower echelon functional elements than the FFOR.

Intra-Unit Troop Control System.

OPFOR control within an echelon also differs from that of the FFOR. For example, Figure 6 shows the composition of a division headquarters staff organization and the key staff elements which interface directly with the Division Commander. The KGB Counter-Intelligence Section, as well as the Military Prosecutor and Tribunal, are shown as connected by broken lines. These elements are not subordinate to the commander. They nominally assist him while remaining subordinate to their own higher authorities.

The Chief of Staff plays a vital management role in all echelons from battalion upward and is second only to the Commander. The Commander may be the strategist-tactician, but the Chief of Staff is practically everything else, including the commander's right-hand man in all command and staff matters. He is the only officer authorized to issue orders in the name of the commander and must have all the qualifications the commander possesses. He also controls those functions that are traditionally referred to as G-2 (Intelligence) and G-3 (Operations) in the U.S. Army. Both leaders are the key nodes or centers of gravity within their respective organizations. The Commander, however, must make all final decisions, reflecting the "one-man management principle." OPFOR Front, Army, and Division headquarters are organized basically along the same lines, differing primarily in size and complexity.

Automated Troop Control and the Decision Cycle.

The Soviet Army has instituted a rather significant theoretical and practical approach to troop control on the modern battlefield. *Automated troop control* consists of the systematic steps taken by the staff in order to perform complex space-time analyses and correlation of forces computations. This process is described as *concept-algorithm-decision* :

- *Concept* deals with the commander's understanding of his assigned mission and his overall plan for executing it;
- *Algorithm* is a systematic decision making procedure which generates a series of options (courses of action) for accomplishing the mission, based on objective data and experience;

- *Decision* is the commander's choice of the single best option from among the other alternatives provided for his consideration.

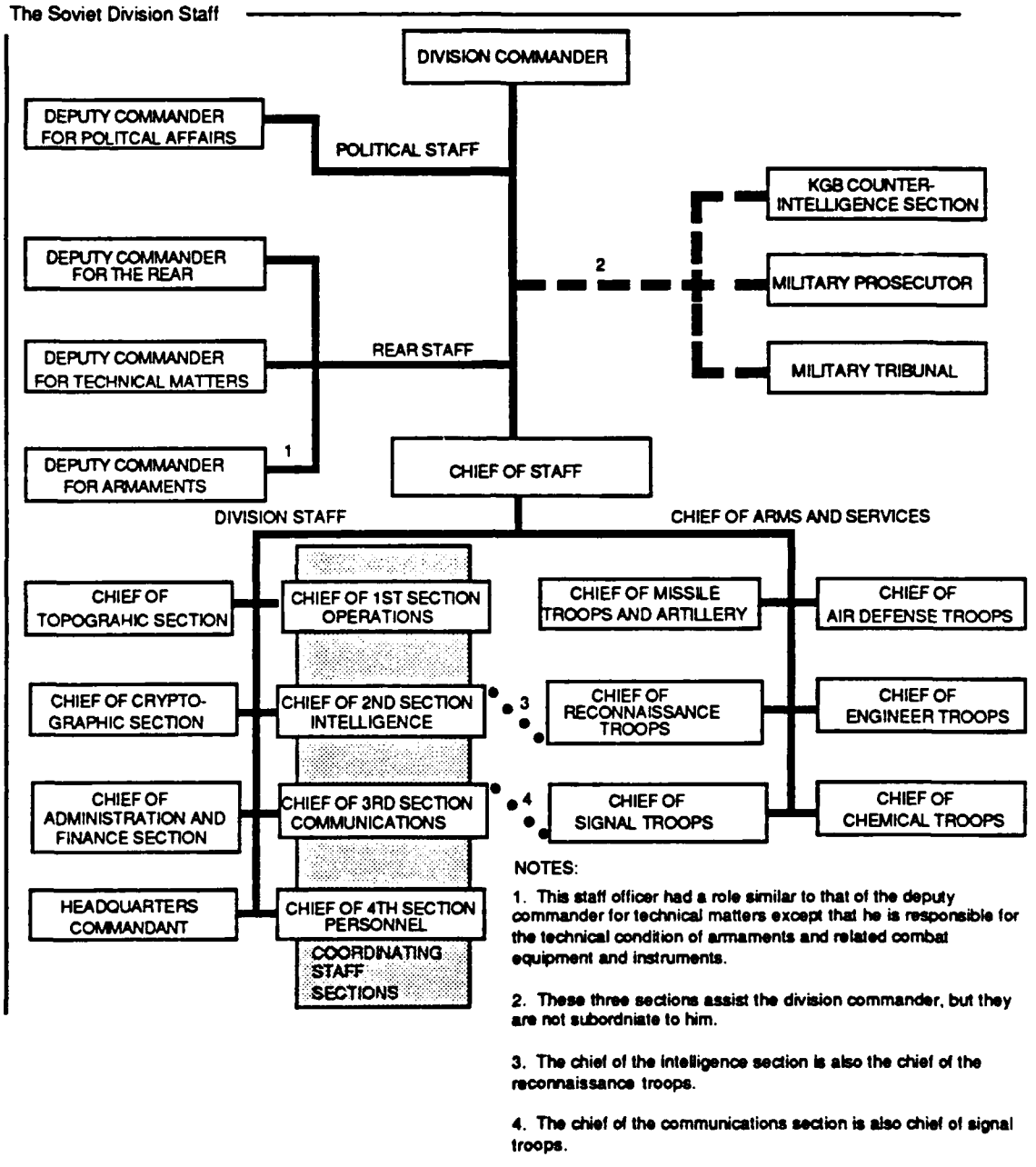


Figure 6. OPFOR division headquarters staff operations.

The decision is considered by the OPFOR to be the basis for planning. Figure 7 simply illustrates the OPFOR's concerns in making a decision. In addition to defining the objective of the combat operations, the decision outlines the forces, resources, procedures and times for accomplishing it. The critical requirement placed on the decision is that it be scientifically sound (Cimbala, 1986). Mathematical methods of operations research and PERT-like planning procedures are among the tools used for this scientific substantiation.

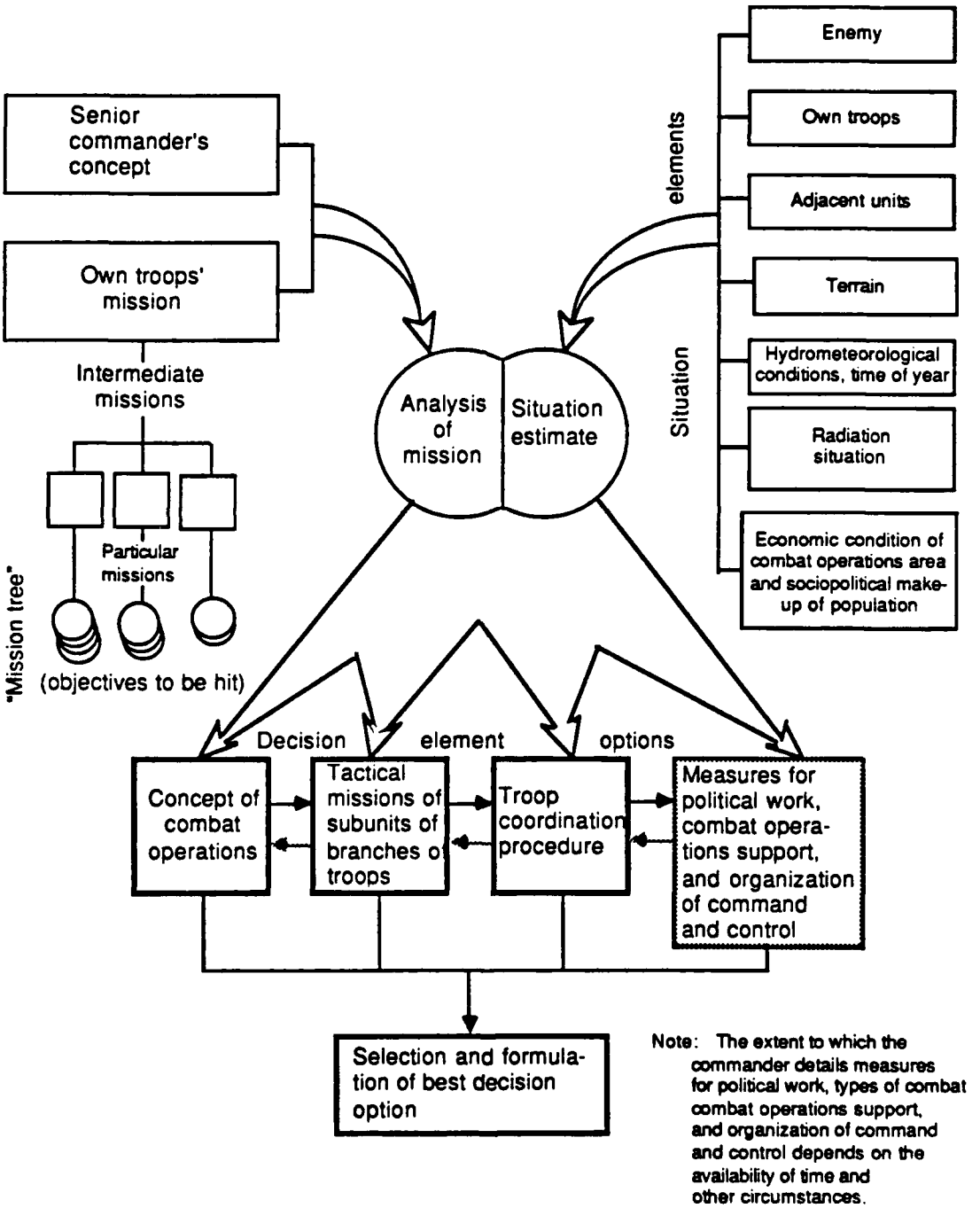


Figure 7. The Commander's decision-making methodology.

The OPFOR decision cycle has surface similarities to that of the U.S. Army, but has a unique ideological approach to its armed force's mission. This approach includes both politically developed doctrine and use of scientifically constructed algorithms for planning and managing battlefield operations.

Network diagrams similar to PERT charts assist in the determination of the most efficient and effective way of allocating tasks throughout the organization and in planning combat operations. This means compiling important factors such as "who is to do what" and "how long it will take to do it." Once completed, these factors are then used to develop a timetable diagram, including:

- the scale of the combat operations;
- the most advisable sequence of actions;
- the best distribution of duties among responsible personnel; and
- time reserves and means of reducing the time consumed for organizing and planning combat operations.

Table 1 shows typical planning operations and the times associated with those operations. The time factor effectively drives the command and control functions and related tasks and activities.

The OPFOR decision cycle is heavily reliant on the commander and his staff in its initial phases. On receipt of the operational or tactical mission from a higher echelon, the commander and staff immediately respond according to their respective responsibilities and functions. One of the first steps in the decision making process is the determination of key situation elements. Figure 8 illustrates the intelligence-reconnaissance function in its role as provider of information and intelligence for determining many of these situation elements. As discussed earlier, this function is continually active in order to maintain an accurate representation of the dynamic and fluid battlefield situation. However, intelligence-reconnaissance collection assets are directed at specific assigned mission targets when a mission order is received and its objectives are known. Figure 8 shows the multiple sources from which essential information about the battlefield situation are collected and acquired by the OPFOR. It is apparent that many "eyes and ears" and sensors provide the commander and staff with a vast amount of information -- not just on the enemy, but on their own forces and the combat environment. It is up to the analytical teams to reduce much of the raw, processed data to meaningful intelligence information that will support the essential situation elements within the established time frame set by the Chief of Staff. These situation elements are shown in the upper right block of Figure 7. The OPFOR commander and control organs distribute the tactical missions to the troops and organize their coordination after adopting the decision and engaging in combat planning.

The OPFOR recognizes several key principles of command and control: scientific approach, one-man management, and centralization. As outlined below, this differs from the FFOR decision cycle in several significant ways.

Table 1. Typical work-operations by commander and control organs: basis for network/pert chart.

Name of operation (in general terms)	Executive agents	Duration of operation in minutes
1	2	4
Analysis of assigned mission by the commander and the chief of staff	Commander and chief of staff	20
Plotting the mission on the second working map	Staff officer	18
Study and estimate the enemy	Staff officer	20
Calculation of time for organizing combat operations (while analyzing the mission)	Chief of staff	7
Giving instructions for preparing data and calculations required to make the decision and for taking measures to prepare the troops for the forthcoming combat operations	Commander	10
Issuing warning order to reconnaissance subunit	Staff officer	5
Issuing warning order to combined arms subunits	Staff officer	12
Issuing warning order to the special troop subunit	Service chief	5
Estimate of enemy	Commander and chief of staff	20
Report to commander of data and calculations on the enemy	Staff officer	10
Analysis of assigned mission	Service chief	10
Developing the calculation of the correlation of forces	Staff officer	20
Participation in developing the calculation of the correlation of forces	Staff officer	10
Assigning mission to reconnaissance subunit	Staff officer	18

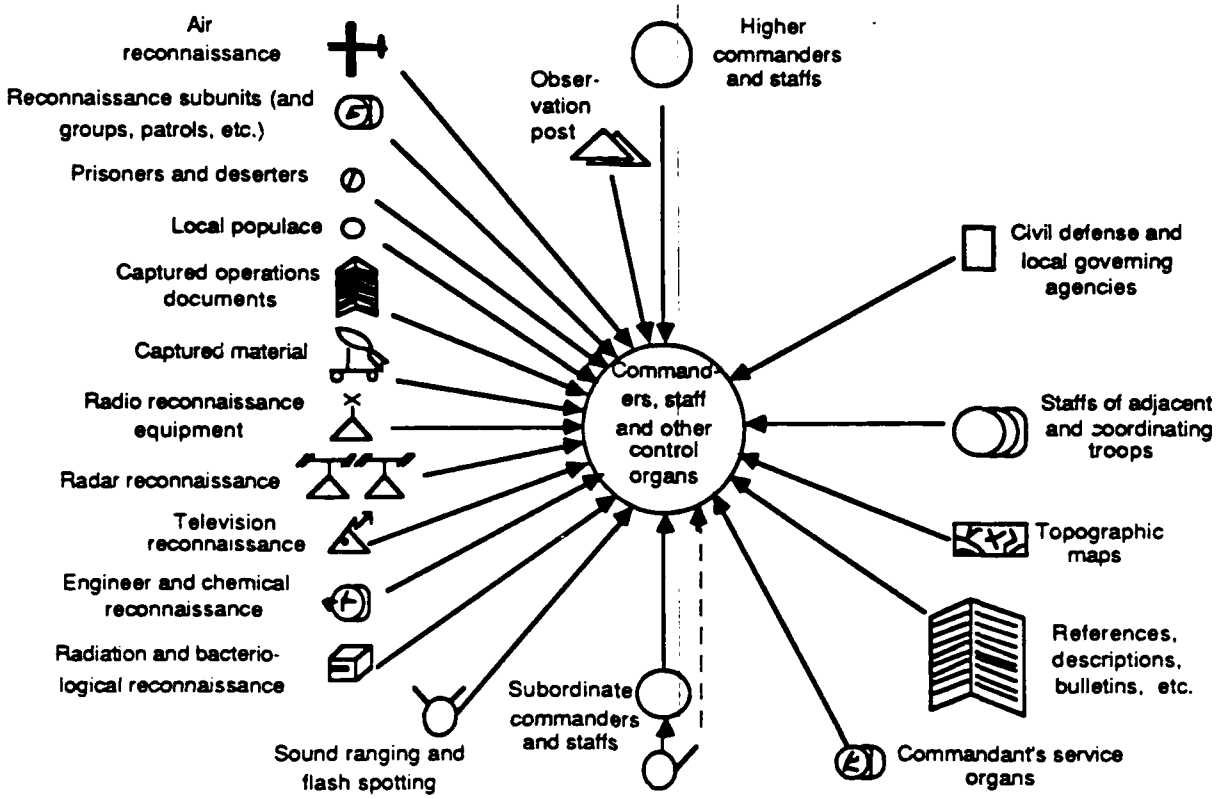


Figure 8. Commander and staff sources for obtaining situation data in combat.

Comparing Decision Cycles

There are eight key general information processing characteristics on which the specific FFOR and OPFOR organizations discussed above can be compared. These eight characteristics and their applicability to these specific FFOR and OPFOR organizations are shown in Table 2. This table also provides implications of these characteristics for the OPFOR's vulnerability to deception. The vulnerability implications are elaborated in the next section.

Centralization is the extent to which tactical decisions are made at high levels and central locations. Operational Homogeneity is the degree of decision making similarity among same-size units (e.g., division) in a force. Algorithmic Reliance refers to the use of mathematical formulas or algorithms to make tactical decisions. Preplanning is the extent to which battle plans (including contingency plans) are formulated well in advance of the battle. The Need for Redundancy reflects the level of confidence a force places on any single source of information. Hi-tech Reliance is the extent of automated or computerized information processing. HUMINT Reliance refers to how much human intelligence is valued. Finally, Risk Preference reflects the force's level of tolerance for uncertain information and plans.

Table 2. General organizational factors affecting vulnerability.

General Characteristic	OPFOR Extent (relative to FFOR)	Implications for Vulnerability
Centralization	High	limited decision-making at lower level
Operational Homogeneity	High	standardization
Algorithmic Reliance	High	predictable and systematic sensitivity
Preplanning	High	reduced real-time decision-making; predictable sensitivity
Need for Redundancy	High	sensitivity depends on interactions between paths
Hi-tech Reliance	Low	hi-tech data channels not used; time delays
HUMINT Reliance	High	human cognitive biases *relevant; time delays*
Risk Preference	Low	hi-risk actions relatively insensitive

ATTACKING THE ENEMY'S DECISION CYCLE

What are the means, method, and criteria for deceiving the enemy?

The purpose of deception is to cause OPFOR actions which lead to the accomplishment of FFOR operational mission goals. To do this, the deception planner tries to induce the OPFOR commander to act in a manner which he would not otherwise pursue. The planner accomplishes this task within the context of available means, by using a deception method, and guided by deception criteria.

Deception Means

Deception means are the resources and options available to the FFOR commander to deceive the OPFOR. They are the building blocks for the deception plan. Deception means can be divided into four categories: tactical actions, personnel, equipment, and deception materiel. This section defines these basics and how they may be used in a deception tactic.

Tactical Actions

A tactical action involves the moving of specific units to certain locations at certain times and with particular plans for future actions (intentions). Any significant change in any of these factors (unit, location, time, or intentions) constitutes a distinct action. As part of a tactical action, measures may be undertaken to inhibit or control the flow of information to the OPFOR (e.g., OPSEC). Tactical actions are usually not strictly deceptive in nature, but may be very effectively used for deception purposes.

The *outcome* of a tactical action refers to the new tactical situation that exists as a result of that action. In a tactical engagement, many factors contributing to the outcome of an action are uncontrollable, unpredictable, or unknown. Thus, an action cannot be predicted to result in a single certain outcome. Instead, an action may be expected to result in one of a number of possible outcomes. The results of this uncertainty are:

- the link between a deceptive measure and an outcome is complex and unpredictable,
- estimates of perceptions, actions, and outcomes are crucial, and
- any information, knowledge, or techniques that can enhance these estimates are very valuable.

The value of a deceptive action must accordingly be determined in terms of its possible resulting outcomes. Some common feature of those possible outcomes must be measured to evaluate the benefits of the action. OPFOR actions must be chosen so that differences between the most likely possible outcomes and the desired situation are minimized.

Personnel

Personnel are the military commander's most flexible and valuable asset, and their proper employment on the battlefield is of critical importance. Personnel may be taken away from their primary duties to perform deception tasks so long as their absence is not detrimental to the overall mission.

Equipment

Materiel that is organically assigned to the unit as part of its TO&E for other than deception purposes is referred to as "equipment". In most cases, some military equipment will be required as part of any deception activity. This equipment could include sophisticated weapons systems used to create a

notional attacking or defending force. It could also be as simple as trucks or personal equipment and weapons to portray a platoon or company headquarters. Even expended, damaged, and unrecoverable equipment can be a deception resource. For example, a forward area supply point can readily be simulated by using empty fuel bladders and expended ammunition boxes and casings. These items can give the illusion of activities or troop concentrations without tying up and risking valuable assets.

Deception Materiel

Deception materiel is equipment that is specifically designed for deception. This equipment might range in sophistication from inflatable decoys which can portray artillery or air defense weapons to "black boxes" which simulate electronic and other signatures. For instance, appropriately camouflaged dummy equipment and a black box to simulate infrared (IR) and electronic signatures can make up a near-complete decoy package without committing actual weapons. The range of options will dramatically increase as deception equipment becomes more readily available.

Deception Method

Development of specific deception strategies requires knowledge of the decision cycle of the OPFOR. This knowledge is required to identify OPFOR vulnerabilities and to formulate a plan of action for selecting and accomplishing the deception mission. To better understand OPFOR decision cycle vulnerabilities, the deception process may be divided into two parts:

- analysis of the OPFOR organization to determine how deception goals could be achieved through a "deception story;" and
- utilization of FFOR resources to convey that deception story to the OPFOR.

There has historically been more focus on the second of these parts. The U.S. Army, as the FFOR, has long developed the capability to affect the OPFOR's receipt of information. Jammers, decoys, and feints, among other capabilities, deny, distort, and misrepresent information to the OPFOR. However, disruption of the OPFOR's information is not deception in itself; it only affects the OPFOR's source data. Effective deception requires plans specifically targeted to manipulate the OPFOR's decision making processes. Uncoordinated disruption of information channels and sources may usefully promote confusion, but generally is not the most effective use of resources. Analysis of the OPFOR organizations is consequently integral to developing a deception story which takes advantage of the specific vulnerabilities of its decision processes.

Vital to this analysis is the concept of an organizational path, a key component of a military organization (e.g., OPFOR). In such an organization, each OPFOR individual or working team can be viewed as a *node* and each communication path between two nodes as a *link*. Decision processes take place at the nodes, while information transfer occurs through the links. Examples of nodes could include a ground surveillance radar operator and a front commander, while an example of a link could be radio communication between them (e.g., that an armored brigade is on the move). An *organizational path* may be defined as a sequence of links and nodes that connects two specific nodes within the organization with regard to a particular piece of information (e.g., brigade moving).

Each organizational path specifies a single route for a specific piece of information to pass between two organizational nodes. Specific pieces of input data may be transformed at intermediate nodes along the path through various perceptual and decision processes. Some paths, in turn, will connect input data links with specific actions (that result from a decision node). Organizational paths consequently present an operational way to interrelate data input, processing, and action. The deception planner uses an understanding of the OPFOR organizational paths to optimize the effectiveness of deception.

Deception Criteria

Criteria are general measures of effectiveness (MOEs) used to evaluate the processes that are important for successful deception. The criteria fall into two groups: those associated with OPFOR tactical actions which are targeted by the FFOR, and those associated with the FFOR deception planning process. These *action* and *plan* criteria are discussed in the following.

Action Criteria

There are four criteria needed to evaluate for deception the actions of the OPFOR: vulnerability, manipulability, exploitability, and desirability. These are discussed in turn.

Vulnerability. Vulnerable actions are those that are susceptible to change based on new input data to the OPFOR decision cycle. If changes in the input data on an OPFOR C2 path lead to altered decisions and actions, those actions are said to be *vulnerable* to deception. Not all actions are vulnerable, of course. In some cases, actions may be preplanned and ballistic and, in others, changes in data may not be carried on any path.

Vulnerability may be assessed only after identifying and assessing all the factors which affect it. Based on generality, there are three classes of vulnerability factors. The most general of these factors are those which affect all tactical organizations in all situations. Called "deception maxims" in FM 90-2, such factors include the Law of Small Numbers, Magruder's Principles, and the Conditioning Maxims. Each of these deal with building and reinforcing a force's tendency to seek and use only that data which *confirms* their current beliefs. Based upon a general knowledge of the OPFOR, the second class of vulnerability factors is referred to as *organization-specific*. These factors are based upon general characteristics of specific force organizations (e.g., centralization and preplanning). They are summarized in Table 3. The third class of vulnerability factors are *situation-specific*. These include specific conditions of the battlefield (e.g., time, FFOR situation, OPFOR situation, weather). Situation-specific factors cannot be analyzed a priori but must be dealt with on the battlefield in real time.

Manipulability. Manipulability is concerned with the FFOR and its ability to apply effective means to OPFOR actions. A n action is considered to be *manipulable* if the FFOR can affect the action by altering the input data to the OPFOR. Manipulability consequently depends on both the OPFOR and the FFOR whereas vulnerability depended only on the OPFOR.

There are many categories of factors which affect manipulability. Of these, the most general category again contains factors which hold true for any tactical organization and are summarized in FM 90-2. The deception maxims that are particularly oriented to manipulability include:

- Axelrod's Contribution -- save a one-shot deception resource until "the time is right";
- Sequencing Rule -- use deception resources in such a way as to maximize the effective duration of the deceptive story; and
- Planned Placement of Deceptive Materiel -- make the target "work" for the deceptive materiel.

The first two maxims deal with the timing of the deceptive means. The third states that a path is more manipulable if the target has to expend considerable effort to obtain or interpret the materiel.

Table 3. Organization-specific vulnerability factors.

Degree of Centralization:	This refers to the extent to which key information processing decisions are made by a central, high-level authority or are distributed and made in parallel. Key decisions here include both sensing/interpreting of information and planning/implementing actions. Highly centralized information processing structures are better able to achieve consistency of response and efficiency of decision making. They are also, however, relatively insensitive to distant localized conditions and unable to rapidly respond to unexpected stimuli. Distributed structures are less able to achieve unified and tightly coordinated action, but are more able to perceive and respond rapidly to local conditions and unexpected stimuli. Both structures pose opportunities for deception.
Degree of Preplanning:	This characteristic refers to the extent to which specific intelligence and operations activities are planned in detail before the engagement begins. Advantages or preplanning are speed and consistency of response; the primary disadvantage is confusion if unanticipated contingencies occur. Organizations with lower degrees of preplanning are initially slower to act. However, they have no anticipations already implicitly built into pre-existing plans and they are more able to act quickly with a broader range of options.
Formalization of Decision Making:	This feature is concerned with the extent to which planning and decision-making are based on formal, standardized methods (e.g., models, formulas, simulations, nomograms) or on individual decision maker criteria and experiences. When standardization and formalization are high, the organization achieves greater consistency, formality, and "rationality". This also makes its behavior more predictable, and can reduce creativity and learning on the part of individual decision makers. Use of individual criteria, on the other hand, can lead to decisions that are inconsistent across units of the organization and problems in coordination of decisions. Individual criteria allow more flexible responses and permit development of more expertise on the part of key decision makers.
Technological Style:	Each command organization will have a general technological style or approach. There may be reliance on: high-tech equipment; preferences for certain types of sensors or weapons; man-machine function allocation; or a general avoidance of such reliance. The technological reliance leads to improved capabilities under nominal conditions, but may lead to degraded performance in highly stressed problematic situations. An avoidance of technological reliance may make the organization more resistant to stress-induced failure, but also generally slows the speed of and capacity for information flow in the organization.
Command and Control Structure:	The nature of the C2 structure -- what functions are linked and how, the degree of redundancy, etc. -- is an important determinant in the vulnerabilities of a force. Highly redundant systems have increased chances of successful communication, but typically allow a smaller variety of messages. Such a system may be susceptible to: overconfidence, if information is sent to distinct channels. Less redundant systems are susceptible to the loss of information or the loss of functionality if key communication links or organizational components are lost.

The organization-specific manipulability factors relate deception means to broad, organizational characteristics of the OPFOR. Conceptually, these factors could lead to "implications for manipulability" (analogous to the implications for vulnerability in Table 3). Each significant organizational characteristic would be analyzed for its implications for utilizing means. For example, reliance on algorithms to guide decisions has vulnerability implications because of the limited range of possible actions resulting from an algorithm's application. The same characteristic has manipulability implications by spelling out the factors considered by the algorithm. Knowing these factors places sharp constraints on the means used: the means must be capable of manipulating the inputs which drive the algorithms. The situation-specific factors are perhaps even more important for manipulability than for vulnerability. The specific tactical situation will determine the manipulable actions by: (1) limiting the OPFOR possible actions; and (2) constraining the deception resources available to the FFOR.

Exploitability. An *exploitable* action is one that is simultaneously vulnerable and manipulable. Vulnerability, it will be recalled, is concerned with actions which can be influenced by changing the input data. Also, manipulability is concerned with means that can manipulate *the same input data* in appropriate ways to achieve a specific OPFOR action. Here, assessing the exploitability of an action requires the analysis of both vulnerability and manipulability and of the interaction between them. Time is the crucial variable for exploitability. For example, a given action may be found to contain a window of vulnerability that is open for the next six hours. If the FFOR possesses the means to exploit this vulnerability, it must be able to mobilize those means within the six-hour window. If it cannot, the action is not exploitable.

Desirability. The above discussions are incomplete without relating these concepts to the reasons for doing the deception (i.e., deception goals). *Desirability* analysis -- determination of the OPFOR actions which lead to a desirable FFOR outcome -- provides this critical link. This analysis examines a given potential OPFOR action for the extent to which that action leads to the desired outcomes. Desirability assessment depends on the commander's mission objective, which is in turn based on the current tactical situation. Unless done in a systematic manner to achieve a desirable result, the practice of deception can be a waste of time and resources. The principal concern in planning a deception operation is to determine the desirability of the anticipated outcome of the deception. Evaluating desirability throughout the planning process increases efficiency by eliminating undesirable results.

Plan Criteria

The two criteria needed to assess a deception plan are verifiability and consistency. *Verifiability* refers to the extent to which the plan can be evaluated in progress, while *consistency* refers to the various ways in which a plan "hangs together".

Plan Verifiability. This broadly refers to the ability of the FFOR to monitor the progress of the plan while it is being executed. The need for this feedback results from the fact that the deception story is unfolding over time to the OPFOR target. As in other kinds of operations plans, the deception plan should have control points built into it which allow the deception operation to be adjusted or redirected. These control points should be logically built around key plan events which correspond to key points in the story. If the target does not move in the desired direction at these key points, the planner should have alternates, revisions, or methods of revision available to correct the problem. This can be done only if the deception cell can obtain information on the progress and status of the plan execution up to that point. There are several concerns which should be examined when assessing verifiability:

- the planner should anticipate key points in the plan and build in means to evaluate the plan's success at these points;
- the planner should seek to obtain feedback from multiple channels and at multiple points in the plan;
- the planner should develop alternative plans at each of these control/verification points; and

- the planner should design the feedback mechanisms to provide enough information for informed choices among possible alternative plans or possible modifications if a plan falls apart.

Plan Consistency. This broadly refers to four kinds of consistency that should be built into a deception plan: breadth, temporal, behavioral, and external.

- *Breadth consistency* -- this is the criterion which deals with the consistency of information across channels of access to the deception target. Consider the two-part principle referred to as Jones' Lemma: "Deception becomes more difficult as the number of channels of information available to the victim increases. However, within limits, the greater the number of controlled channels, the greater the likelihood of the deception being believed" (ORD,1981, p.21). The planner must insure consistency of information across all controllable channels, and revise the plan if this consistency is not found.

- *Temporal consistency* -- this is the property that deals with the believability of different temporal parts of the plan with regard to each other. A deception story unfolds over time. Because of the extended duration of the deception operation, it is necessary to convey distinct pieces of information at different times over the entire duration of the deception activity. The *timing* of these information items must make sense to the OPFOR. Maximizing the believability of the deception story will require the planner to segment the plan into different phases which unfold consistently over time.

- *Behavioral consistency* -- this refers to the believability of the entire deception story, in light of previous behavior by the deceiver. It is a well-known lesson of warfare that to "know the enemy" is a critically important requirement for a tactical commander. The essence of this knowledge is to be able to see the world (viz., the tactical battlefield) through the eyes of the adversary. In this light, the OPFOR commander will look at any (real or notional) operation of the FFOR and ask, "does this operation make sense in relation to previous operations?" Behavioral consistency ensures an affirmative answer to this question.

- *External consistency* --- this refers to the broader operational context in which the deception plan is to be executed. Because the deception plan is only part of the operations plan, it must be coordinated with other operational activities. This coordination is especially crucial with respect to battlefield intelligence collection, other C3CM activities, and any other operational activity in an area where the deception action is to be played out. Coordination must also be achieved with higher-echelon deception and operational actions. Uncoordinated FFOR action can easily blow an otherwise effective deception.

Consistency and coordination should not be looked upon as absolutes. To assess the various kinds of consistency requires both time and other resources, which typically are in short supply. Thus there is a trade-off between the level of consistency and the resources expended to achieve that level of consistency. It is not necessary to achieve absolute consistency, but rather to present appropriately selected information which confirm the preconceptions of the OPFOR.

ENHANCING THE DECEPTION PLANNING PROCESS

How can the steps in the deception planning process be achieved?"

The current deception planning process is presented as deception doctrine in FM 90-2. Figure 9, based upon this field manual, shows the six steps of the current planning process. These steps indicate *what* is to be done with little explanation of *how* it is to be done. Enhancements to the current deception planning process are provided in the following, based upon the analyses in the previous section.

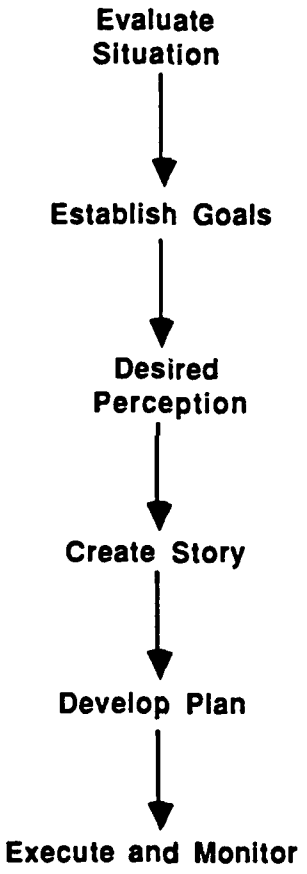


Figure 9. Current Planning Process (FM 90-2).

Enhanced Deception Planning Process

Figure 10 shows enhancements to the steps in the current planning process (original steps denoted by shaded boxes). These enhancements are accomplished by inserting additional steps and constructing feedback loops, if some of these steps prove unworkable. For example, once a goal is established, a targeted decision maker must be identified. If this presents problems, the process flows back to review goals. The enhanced set of planning steps illustrates the process of assessments and tradeoffs that the planner must make.

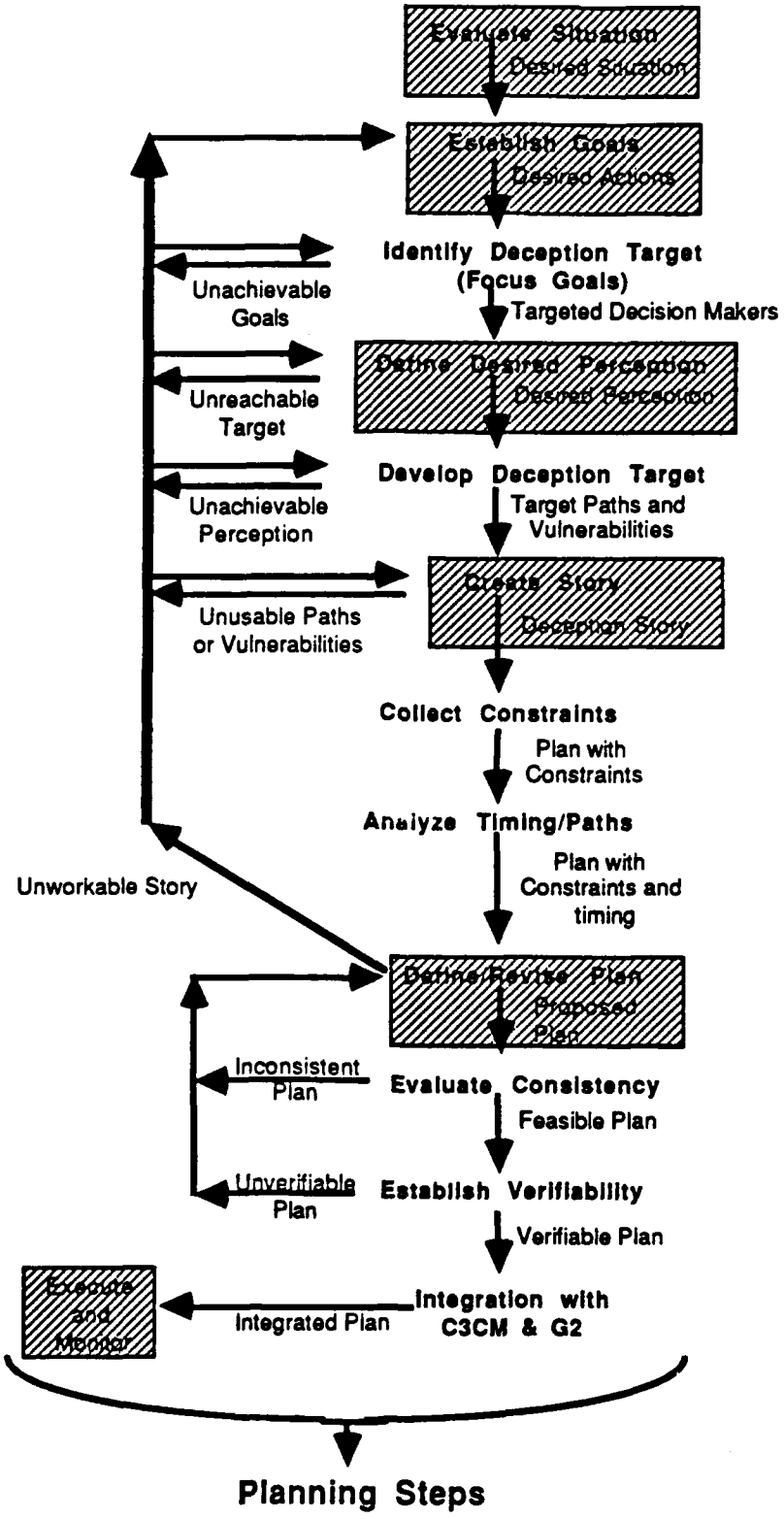


Figure 10. Overall deception planning procedure.

The successful execution of the processing steps requires drawing upon or creating many supporting knowledge and data bases. This may be seen, for example, considering the fifth step in

Figure 10 ("Develop Deception Target"). This step begins with the desired perception which the deception planners want the targeted OPFOR decision makers to hold. The judgment is that such a perception will cause OPFOR decision makers to act in line with FFOR goals. Finding and analyzing the possible paths for establishing the desired perception in the minds of the targeted decision makers follows. The goal of this process -- referred to as*pathfinding* -- is to identify and evaluate the vulnerabilities of each path to deceptive manipulation.

Figure 11 presents the enhanced planning process paralleled by the *knowledge and data requirements at each stage*. Temporal conditions and constraints are particularly important for vulnerability analysis. For example, the centralization of the OPFOR organization indicates that many key decisions are made at higher echelons, each having longer-range planning and decision windows. If the FFOR can compress the available time in a manner not preplanned by the OPFOR, the entire decision cycle may be disrupted. Not only may windows become shortened, but some operational nodes and links could be eliminated or distorted. The OPFOR uses a systematic temporal structure for its tactical decision cycle which becomes increasingly vulnerable as response time is compressed. The vulnerabilities analysis depends on the analysis of constraints arrived at through pathfinding.

Pathfinding requires a great deal of knowledge about the OPFOR. First, it requires knowledge about his intelligence collection, communication, and analysis system. In addition, it requires understanding of the system by which the targeted OPFOR decision makers receive, evaluate, and act on information and intelligence about the situation. In addition to knowledge requirements, several factors constrain the pathfinding process:

- capabilities and limitations of FFOR and OPFOR in personnel, training, materiel, combat service support, combat support, and application of combat power;
- time constraints imposed on and by FFOR and OPFOR (i.e., planning horizons, reaction times of decision cycles, etc.);
- FFOR and OPFOR mission objectives and ways and means of achieving those objectives;
- beliefs of FFOR and OPFOR about each other and what the other would do in a given situation; and
- the range of resources, personnel and time available for use by FFOR deception planners.

Pathfinding is a means for deception target development which builds on OPFOR decision making vulnerabilities. These are the vulnerabilities implicit in the analyses of the information environments in which the targeted decision makers are working. They are also implicit in the statement of the desired perceptions which they must hold if they are to execute the desired actions. Pathfinding attacks the targeted decision makers by attempting to find potential ways to manipulate their decision environment (via their available intelligence and knowledge). The purpose of this manipulation is to significantly increase chances that the OPFOR will execute the desired actions and thus bring about the desired situation for the FFOR.

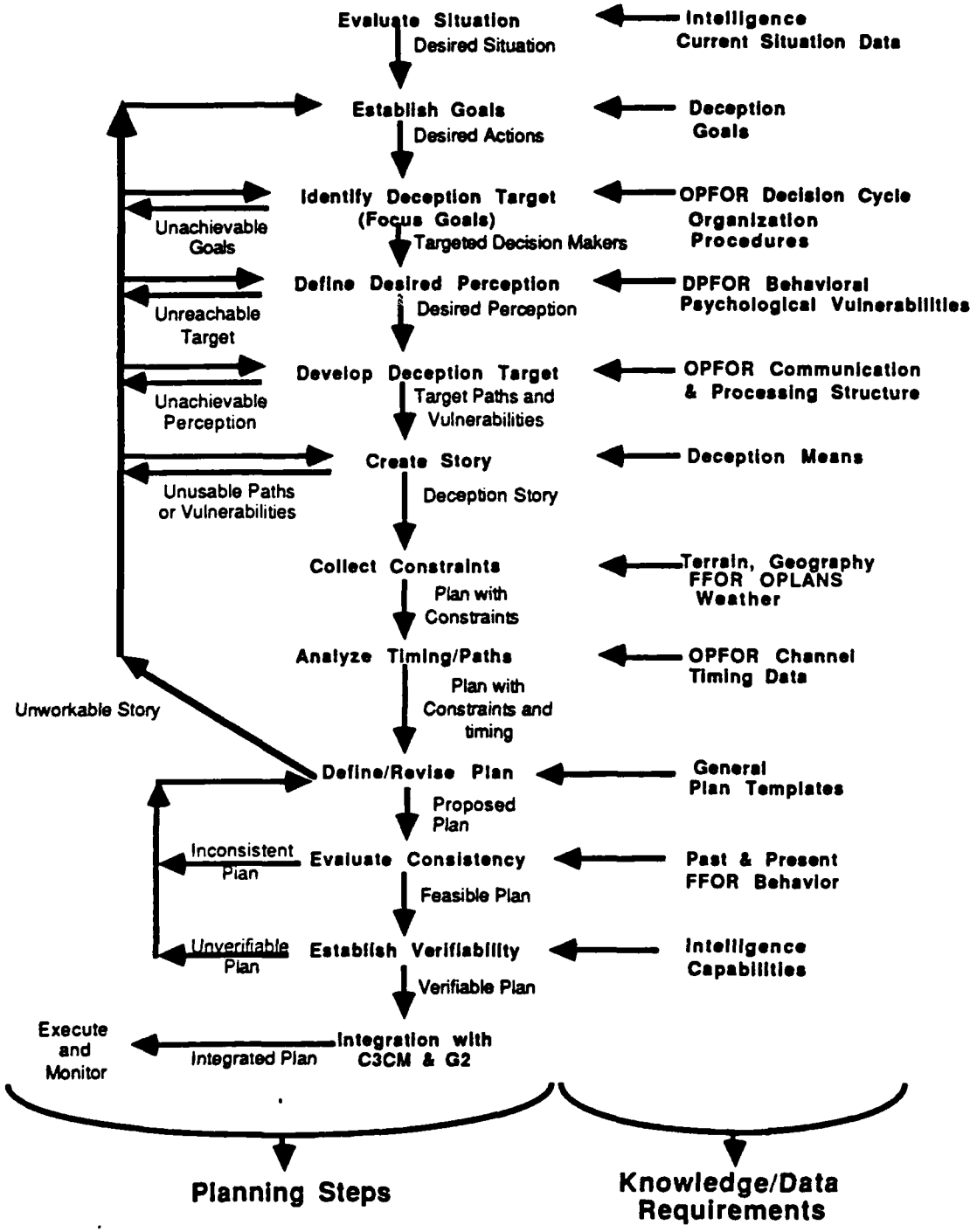


Figure 11. Overall deception planning procedure with knowledge/data requirements.

DOING DECEPTION: APPLYING PATHFINDING TECHNIQUES

How can pathfinding be applied to a tactical situation?

The following two examples illustrate how pathfinding might be applied in a conflict between US/NATO and Soviet/Warsaw Pact. Based on the goal of changing the targeted decision maker's situational beliefs, the examples demonstrate how the planner might use pathfinding. Both examples deal with only a single step in the deception planning process -- identifying and developing vulnerable paths to the targeted OPFOR decision maker. Each example ends with a graphic representation of such paths, called a *Partial Path Space Diagram.* The scenario is adapted from the TRADOC Common Teaching Scenario (TRADOC, 1985).

Pathfinding Example 1: Multiple Reinforcing Paths Within a Given Echelon

A Central European confrontation has developed with the expectation of an OPFOR attack across the Inter-German Border in several days. The deception cell has been tasked to produce a deception plan to support Contingency Plan (CONPLAN) DARBY based upon the anticipated situation 24 hours after this attack (i.e., D + 1). The anticipated tactical situation triggering execution of DARBY is depicted on the map in Figure 12. The planning has therefore provided descriptions of desired battlefield situations:

Enemy Situation.	Lead elements of the 1st Echelon divisions of an OPFOR Combined Arms Army are expected to cross the Inter-German Border and engage US covering forces in the Fulda Gap. The 8th Combined Arms Army (8 CAA) is expected to attack the northern portion of the 10th (US) Corps sector, possibly driving north of Lauterbach and south of Alsfeld. Figure 12 shows an overview of where the various forces are expected to be deployed at approximately D + 1. The advance of the 79 Tank Division has been significantly slowed through efforts of the 10th Combat Aviation Brigade (10 CAB). The 79 Tank Division is not expected to be in the Fulda River vicinity until D + 2.
Friendly Situation.	The 10th (US) Corps CONPLAN DARBY is being formulated to deal with the possibility of significant success of the 8 CAA in penetrating through the lines of the 23rd Infantry Division (Mechanized) in the LAUTERBACH - ALSFELD area. A deception plan is being formulated to facilitate the use of this CONPLAN. The deception planning process is at the stage of developing the target (cf., Figure 11). The products of the earlier steps in the planning process are summarized below.
Desired Situation:	OPFOR main effort in northern part of 10 (US) Corps sector, facilitating our use of corps counterattack plan DARBY (with the FFOR 313 unit attacking along AXIS DOG).
Desired Actions:	OPFOR directs main effort toward northern part of sector.
Targeted Decision Maker:	Commander, 8 Combined Arms Army.
Desired Perception:	10 (US) Corps Tactical Command Post (CP) deployed in 52nd Infantry Division (Mechanized) sector, implying that main (US) effort will be in the southern part of 10 (US) Corps sector.

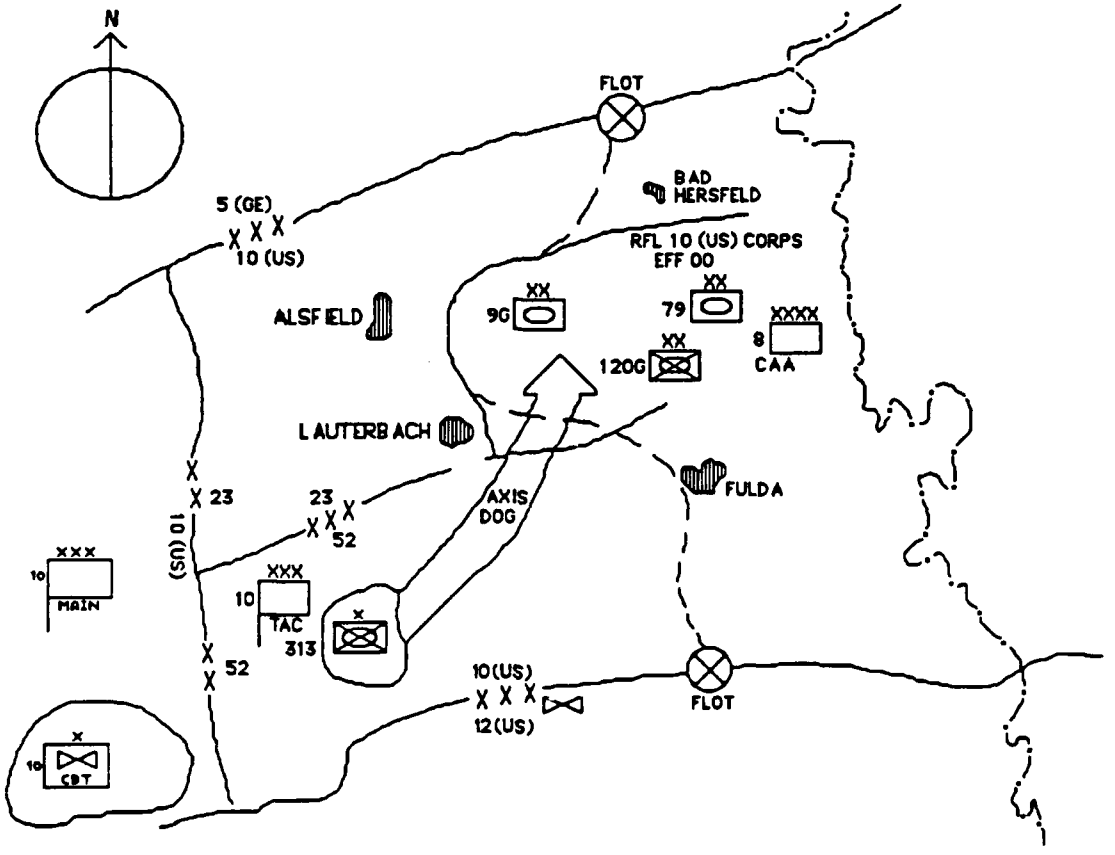


Figure 12. Example tactical map.

Identification of information paths connecting sensory inputs with desired actions can begin once the targeted decision maker has been identified and the desired perception has been determined. One way to approach this task is to identify the possible sources of information coming into the targeted unit, as depicted in Figure 13 for the 8 CAA. Actual identification of all possible sources of information available to a targeted unit will require detailed analysis of the specific OPFOR organization. This analysis can best be conducted with the use of a model of the OPFOR organization consisting of many interconnected diagrams similar to Figure 13.

The 8 CAA receives information from three sources:

- from units in general support (e.g., 5 Long-Range Reconnaissance Company and 75 Radio & Radar Intercept Battalion) as well as from subordinate maneuver units (e.g., 120 Guards Motorized Rifle Division);
- from superiors in the chain of command (e.g., 2 Western Front, not shown in the figure); and
- from adjacent armies and from elements of the second echelon (e.g., 1 Guards Tank Army, not shown in Figure 13).

The 8 CAA may therefore be expected to receive similar or overlapping information about its area of interest from many diverse sources.

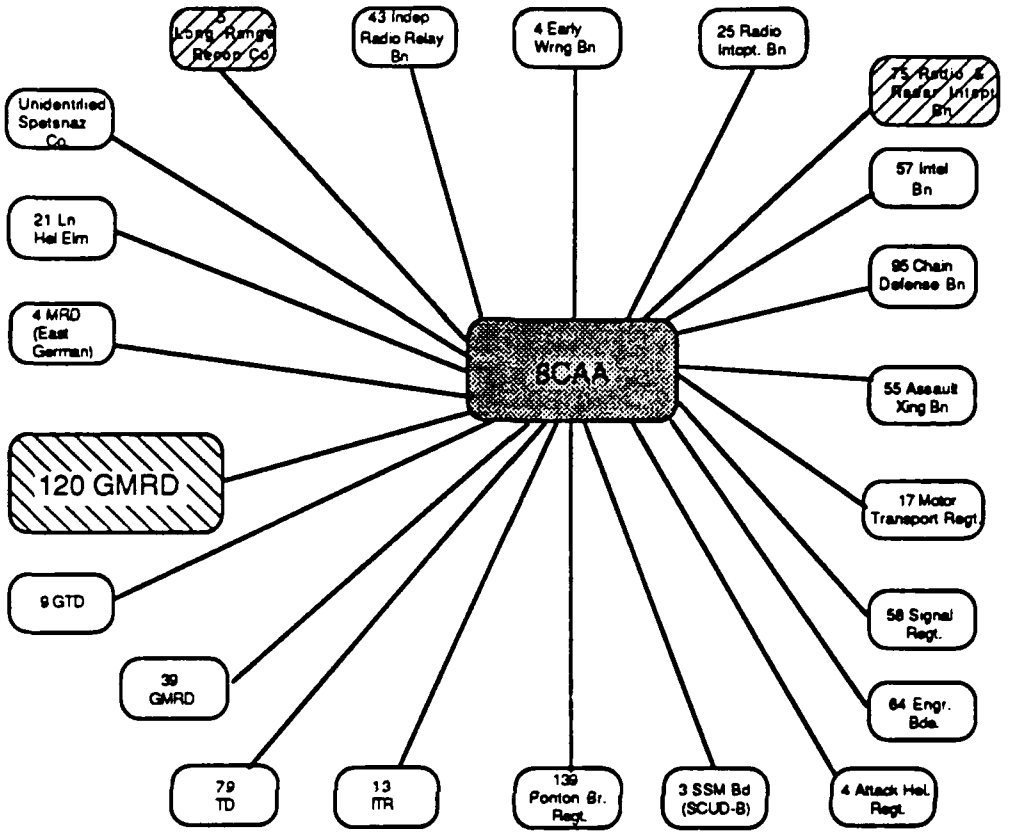


Figure 13. 8 Combined Arms Army, subordinates, and assets in general support.

Analysis of the targeted decision maker's environment can proceed once the information paths to his unit have been identified (i.e., the 8 CAA). The nodes and links comprising this environment are shown in Figure 14. This figure shows that the 8 CAA Commander receives information from his Chief of Staff, his Chief of Missile Troops and Artillery (CMTA) and his Chief of Reconnaissance (RECON); his immediate superior (2 Western Front Commander); and his subordinate maneuver unit commanders (e.g., 120 GMRD). It is important to note that he also coordinates with the commanders of adjacent units, although not explicitly shown.

Figure 13 earlier showed that two key units were likely to pass information about a suspected CP location to 8 CAA Commander through his Chief of Reconnaissance. These are the 75 Radio & Radar Intercept Battalion, and the 5 Long-Range Reconnaissance Company. In particular, the 75 Radio & Radar Intercept Battalion will likely notify the Chief of Reconnaissance of:

- increased message traffic consistent with the 10 (US) Corps Tactical Command Post likely deployed in or near the 52 Infantry Division (Mechanized) sector.

In addition, the 5 Long-Range Reconnaissance Company will likely notify the Chief of Reconnaissance of:

- radio direction finding indicates high volume emitter consistent with the 10 (US) Corps Tactical Command Post definitely located within the 52 Infantry Division (Mechanized) sector, and

- ground vehicle and helicopter traffic in the 52 Infantry Division (Mechanized) sector consistent with the 10 (US) Corps Tactical Command Post deployed in area.

Information paths for these three observation/sensor reports (depicted as bold arrows) are shown in Figure 15. Paths to adjacent units are not shown for sake of clarity.

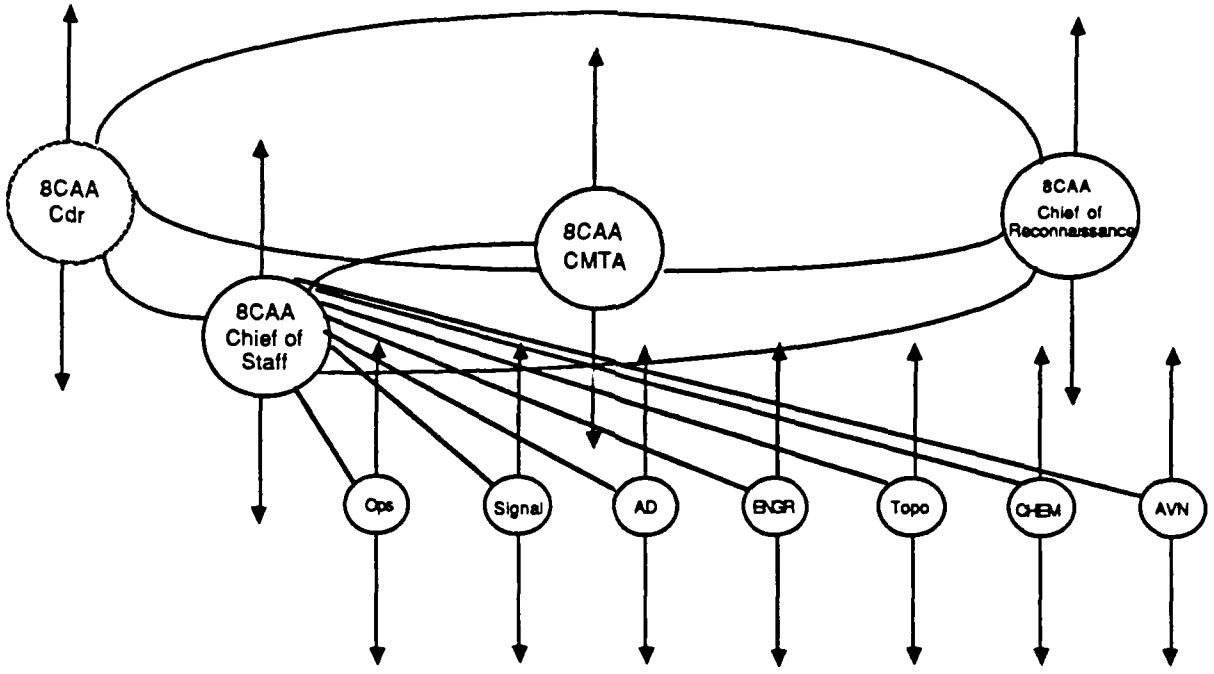


Figure 14. 8th CAA decision environment.

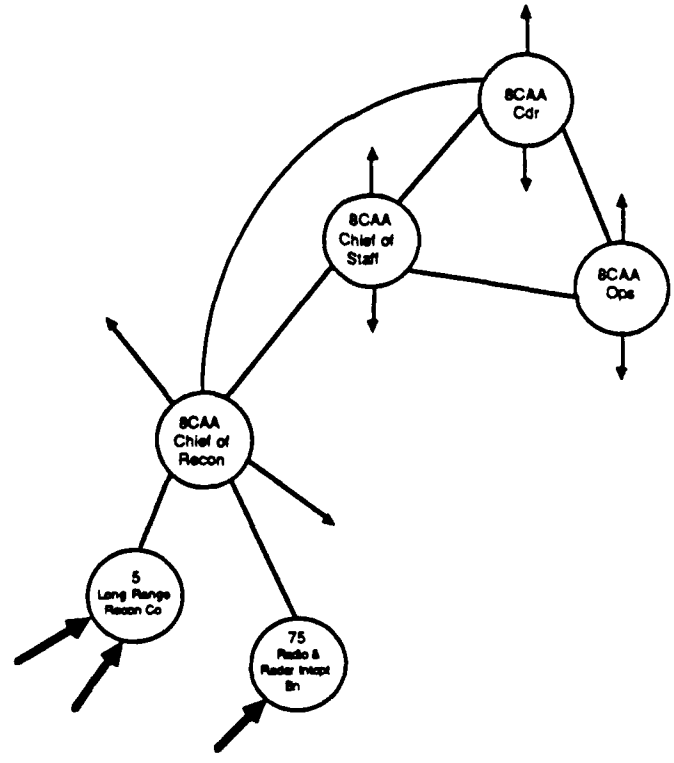


Figure 15. Example 1 partial path space diagram.

Pathfinding Example 2: Multiple Competing Paths Through Multiple Echelons

This second example is based on a scenario for a Central European confrontation which has developed several days before "D" day.

Enemy Situation.	Lead elements of the 1st Echelon divisions of an OPFOR Combined Arms Army are expected to cross the Inter-German Border and engage US covering forces in the Fulda Gap, as in Example 1.
Friendly Situation.	The 10th (US) Corps Contingency Plan DARBY is being formulated to deal with the possibility of significant success of the 8 CAA in penetrating through the lines of the 23rd Infantry Division (Mechanized) in the LAUTERBACH - ALSFELD area (again as in Example 1). However, the deception planning process is at the stage of developing the target (cf., Figure 10). The products of the earlier steps in the planning process are summarized below.
Desired Situation:	OPFOR main effort in northern part of 10 (US) Corps sector, facilitating our use of corps counterattack plan DARBY.
Desired Actions:	OPFOR directs main effort toward northern part of sector.
Targeted Decision Maker:	Commander, 8 Combined Arms Army
Desired Perception:	313 Separate Infantry Brigade (Mechanized) -- the corps reserve -- deployed in 52 Infantry Division (Mechanized) sector, implying that main (US) effort will be in the southern part of 10 (US) Corps sector.

This example expands the scope of the first pathfinding example through the inclusion of likely paths for information flowing up through subordinate units (lower echelons) into the 8 CAA. In particular, this example focuses on the 120 Guards Motorized Rifle Division (120 GMRD), one of the subordinate maneuver units of the 8CAA. The 120 GMRD has an organic Reconnaissance Battalion (Recon Bn) and the 21 Artillery Regiment (21 Arty Rgt) with an organic Target Acquisition Battery in general support. The information from these units concurs with the information from the 5 Long-Range Recon Co and 75 Radio & Radar Intcpt Bn regarding the location and disposition of the US 313 Separate Infantry Brigade (313 Sep Mech Bde). Figure 16 depicts the possible sources of information coming into the 120 GMRD. Figure 17 shows the nodes and links which comprise the decision environment for the targeted unit, the 120 GMRD.

However, once the 313 Sep Mech Bde turns north, the 120 GMRD units which are responsible for southern flank will detect the turn first. This is because: (a) they're more likely to be in the area where the 313 Sep Mech Bde turns, and (b) their job is to protect the flank, which the 313 Sep Mech Bde is going to attack. Thus, conflict between sources available to the 8 CAA and sources available to the 120 GMRD is likely to develop near the time of the turn. The 8 CAA sources are likely to detect that turn later than the 120 GMRD. The 10 (US) Corps must delay discovery of these intentions as long as possible to achieve the deception objective. The information paths for carrying deceptive reports on the position and intentions of the 313 Sep Mech Bde to the 8 CAA Commander are shown in Figure 18 which is an elaboration of Figure 15, the example 1 path diagram. This figure shows a path space diagram which portrays the principal nodes and links which need to be understood to evaluate the vulnerabilities of the 120 GMRD in this particular situation.

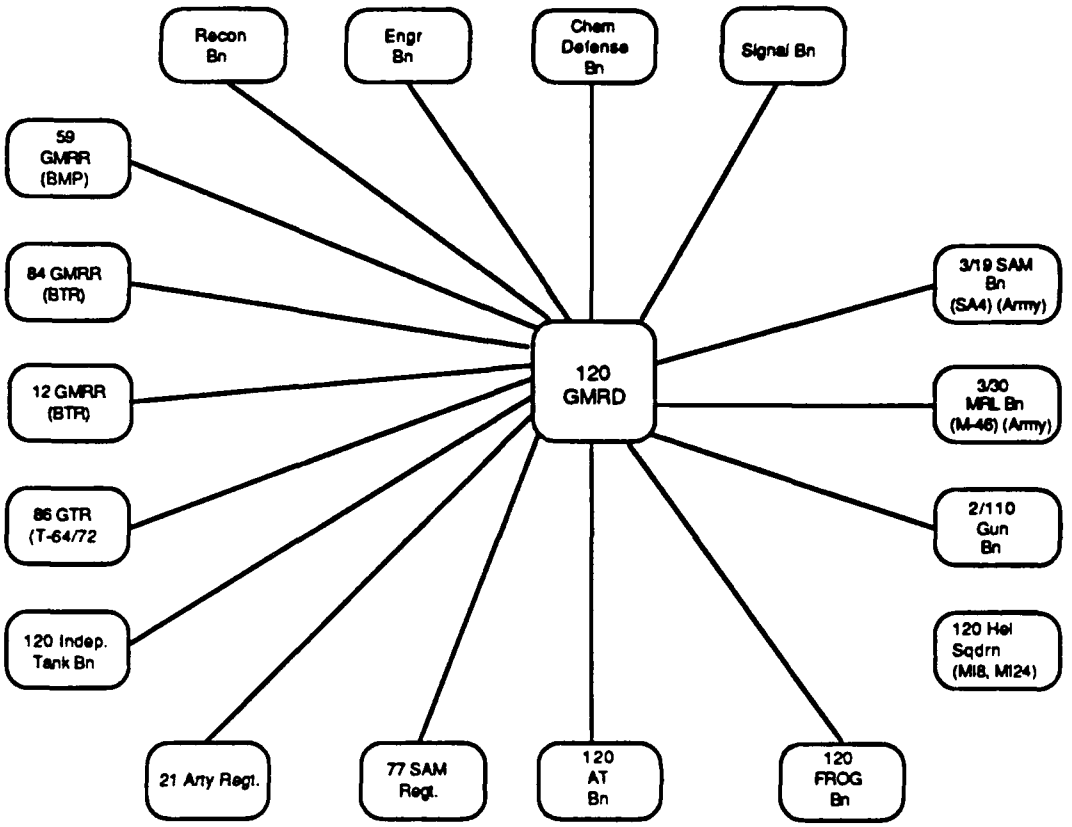


Figure 16. 120 Guards Motorized Rifle Division, subordinates, and assets in general support.

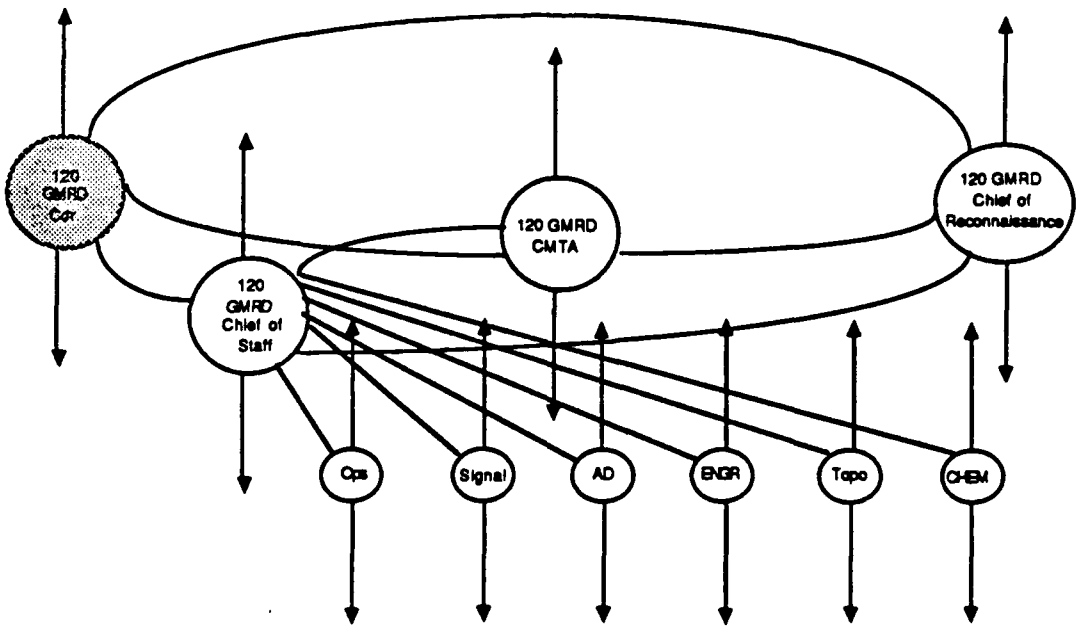


Figure 17. 120 GMRD decision environment.

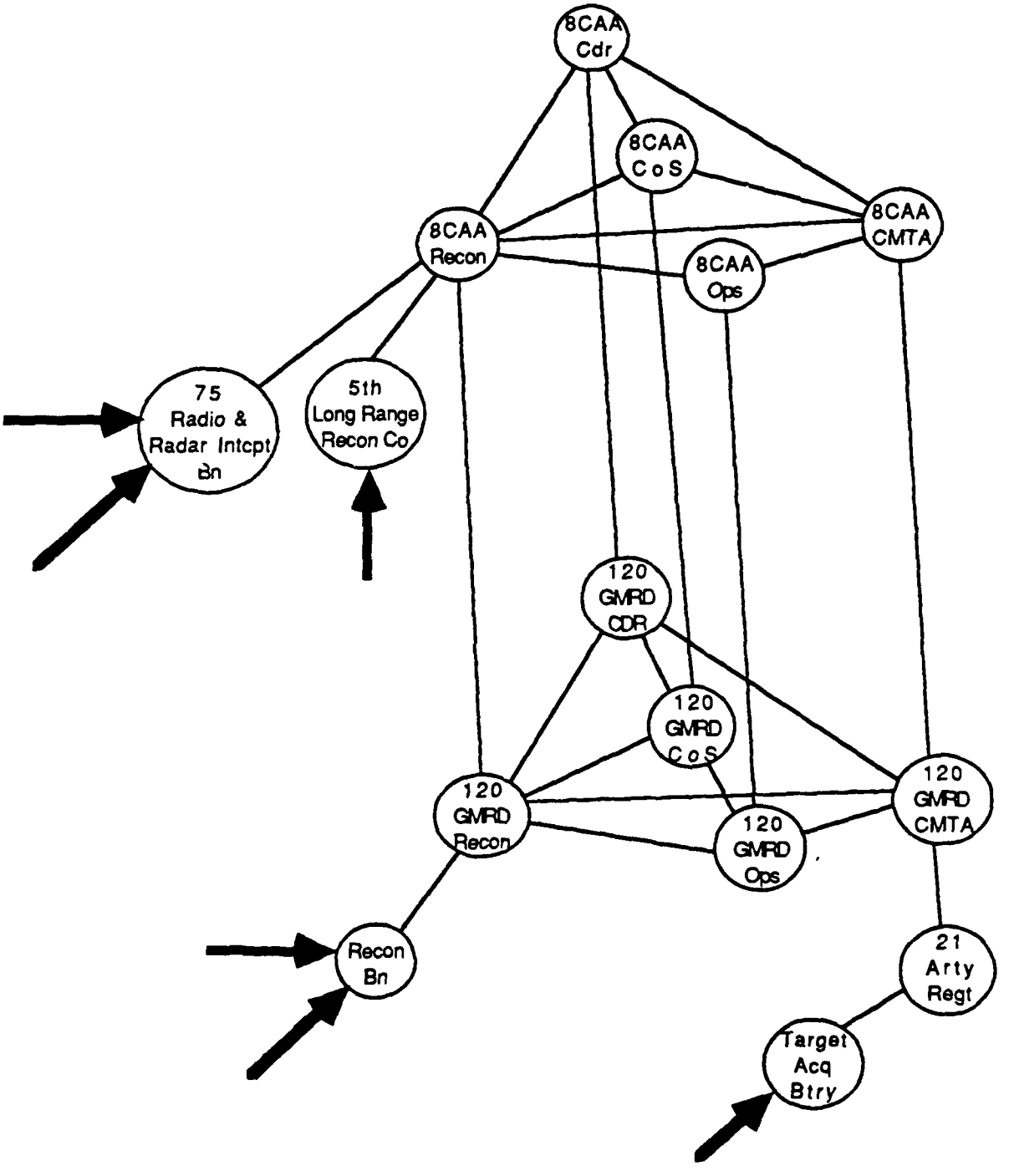


Figure 18. Partial path space diagram.

SUMMARY AND CONCLUSION

This report developed the concept of battlefield deception and constructed an enhanced deception planning process which builds upon current doctrine (FM 90-2). Before developing the enhanced planning process, the FFOR and OPFOR decision making cycles were outlined and contrasted. Next, the means, method, and criteria of the deception planning process were introduced. A key concept arising from this foundation was that of "pathfinding". It was seen that, through pathfinding, the vulnerabilities in the OPFOR decision making cycle may be found and exploited by the deception planner. Pathfinding was seen to enhance the deception planning process by pointing out where the decision making of the OPFOR may be most effectively manipulated. Two illustrations of deception pathfinding were presented in the context of an OPFOR attack across the Inter-German Border. As is evident from these examples, an essential element of pathfinding is "knowing the enemy". Without this in-depth knowledge, vulnerabilities cannot be identified and paths cannot be exploited. Pathfinding and the entire enhanced deception planning process were shown to depend on understanding the enemy's decision making process.